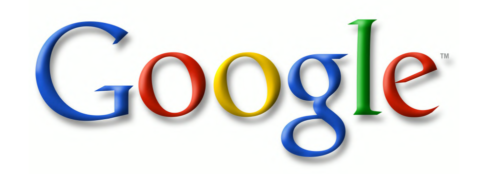
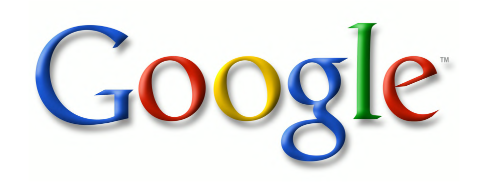


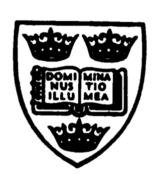



1800
d.50.


600015168R


E. BIBL. RADCL.




DOMI NUS ILLU
MINA TIO MEA

INTRODUCTION

A LA

THÉORIE DES NOMBRES.

PARIS. — IMPRIMERIE DE MALLET-BACHELIER,
Rue de Seine-Saint-Germain, 10, près l'Institut.

INTRODUCTION

A LA

THÉORIE DES NOMBRES,

PAR

V.-A. LE BESGUE,

CORRESPONDANT DE L'INSTITUT (ACADÉMIE DES SCIENCES), PROFESSEUR HONORAIRE DE LA FACULTÉ DES SCIENCES DE BORDEAUX, CHEVALIER DE LA LÉGION D'HONNEUR.

PARIS,

MALLET-BACHELIER, IMPRIMEUR-LIBRAIRE

DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES,

Quai des Augustins, 55.

1862.

AVERTISSEMENT.

Les excellentes *Recherches arithmétiques* de Gauss et la traduction de cet ouvrage étant épuisées, la *Théorie des Nombres* de Legendre étant aussi devenue rare, il m'avait semblé qu'il serait utile de rédiger un nouveau Traité présentant à peu près l'état actuel de la science des nombres. Dès 1858, en cessant mes fonctions de professeur à la Faculté des Sciences de Bordeaux, j'avais pris la résolution de consacrer mes loisirs à ce travail. Je publiai alors des *Exercices d'Analyse numérique,* et j'annonçai la publication par souscription de l'ouvrage en question. Le petit nombre des souscripteurs n'ayant pas permis de donner suite à cette intention, j'y avais renoncé avec regret, quand le prince A. de Polignac, qui s'occupe lui-même de recherches numériques, comme on peut le voir par les *Comptes rendus des séances de l'Académie des Sciences,* a bien voulu éloigner la plupart des obstacles qui m'arrêtaient. Ma reconnaissance pour ce service sera sans doute partagée par tous ceux qui, comme le prince, pensent qu'une exposition claire de l'état présent de la science des nombres, surtout dans ce qu'elle a de bien établi, ne peut manquer de servir aux progrès des mathématiques pures.

L'introduction suivante à la *Théorie des Nombres* contient les propositions élémentaires sur les nombres tant composés que premiers. La théorie des restes des nombres en progression arithmétique donne le moyen de construire une Table pour la décomposition des nombres en facteurs premiers. La théorie des restes des nombres en progression géométrique conduit à la théorie des *racines primitives* et des *indices* ou autrement à la théorie des logarithmes pour un module donné (*logarithmes*

modulaires). De là se déduit la construction du *Canon arithmeticus* de Jacobi ou Tables logarithmiques et anti-logarithmiques. Ces Tables sont réduites de moitié et l'usage en reste presque aussi facile. Cette introduction sera suivie de Mémoires sur les diverses parties de la Théorie des Nombres. Ces Mémoires, réunis et enrichis de tout ce que les deux premiers volumes de l'édition complète des ouvrages de Gauss présenteront de nouveau sur les nombres, formeront un Traité où les Mémoires de Jacobi, Lejeune-Dirichlet, Eisenstein, Cauchy, etc., seront mis à profit, aussi bien que ceux de quelques géomètres qui s'occupent encore de questions relatives à la Théorie des Nombres, ne la regardant point comme une étude de pure curiosité.

INTRODUCTION

A LA

THÉORIE DES NOMBRES.

L'objet de cette Introduction est l'exposition de deux Classifications des Nombres, qui donnent lieu à deux Tables importantes quand on passe de la théorie à la pratique. On y trouvera de plus tout ce qui est nécessaire pour éviter, par la suite, quelques digressions qui auraient rompu l'enchaînement naturel des propositions.

En voici le contenu :

CHAPITRE I. — Objet de la Théorie des Nombres. — Deux classifications principales des nombres. — Exemples de propriétés générales des nombres.

CHAPITRE II. — Des nombres composés. — Permutations. — Nombres figurés. — Arrangements, combinaisons. — Puissance du polynôme, du binôme. — Nombres polygones.

CHAPITRE III. — Des diviseurs des nombres. — Caractères de divisibilité. — Recherche du plus grand diviseur commun à deux ou plusieurs nombres. — Recherche du moindre multiple de plusieurs nombres. — Propriété fondamentale des nombres premiers entre eux. — Restes des nombres en progression arithmétique. — Fractions continues.

CHAPITRE IV. — Des nombres premiers. — De la décomposition des nombres en facteurs premiers. — Théorèmes élémentaires.

CHAPITRE V. — Des Fonctions entières à une seule variable. — Fonctions entières homogènes. — Propositions élémentaires.

CHAPITRE VI. — De la congruence des nombres. — Théorèmes élémentaires.

CHAPITRE VII. — Des restes des nombres en progression géométrique. — Théorie des Logarithmes modulaires ou pour un module donné. — Tables ou *Canon arithmeticus* de Jacobi.

Les propositions énoncées dans les six premiers chapitres étant bien connues, les démonstrations ne sont qu'indiquées, ou présentées sommairement. Pour plus de détails à ce sujet, on peut consulter le *Complément des Éléments d'arithmétique* de M. Lionnet, professeur au Lycée Louis-le-Grand.

Le chapitre VII est plus développé, il expose une théorie qui a beaucoup de rapport avec celle des logarithmes et qui n'est pas moins utile.

Cette Introduction peut servir de *Commentaire* à la première Section des *Disquisitiones arithmeticæ* de Gauss, et à une partie des Sections II et III.

Voici l'explication de quelques signes particuliers à la Théorie des Nombres :

$E(x)$. Ce signe représente l'entier égal ou immédiatement inférieur au nombre réel x. Ainsi $E\left(\frac{7}{3}\right) = 2$, $E(\sqrt{8}) = 2$, $E(\sqrt{9}) = 3$.

$\equiv$. Ce signe, placé entre deux nombres a, b, montre qu'ils sont compris dans une même formule $mx + r$, où m (module) est un nombre donné. L'égalité des restes de a et de b divisés par le *module* m est ce que l'on nomme la *congruence* des nombres a et b pour le module m.

On l'indique par $a \equiv b$, mod. m, qui se lit a congru à b pour le module m. Cette sorte d'équation revient à dire que $a - b$ est divisible par m.

$D(a, b)$, $D(a, b, c)$, etc., indiquent le plus grand commun diviseur de deux nombres, trois nombres, etc.

$D(a, b) = 1$ montre que a et b sont premiers entre eux.

$m(a, b)$, $m(a, b, c)$, etc., indiquent le moindre multiple de deux nombres, trois nombres, etc.

CHAPITRE PREMIER.

OBJET DE LA THÉORIE DES NOMBRES. — DEUX CLASSIFICATIONS PRINCIPALES DES NOMBRES. — EXEMPLES DE PROPRIÉTÉS GÉNÉRALES DES NOMBRES.

1. On entend par Théorie des Nombres la partie des mathématiques pures, qui a pour objet la recherche et l'exposition des propriétés générales des nombres entiers. Le titre de Recherches théoriques et pratiques sur les nombres conviendrait mieux, d'autant plus que c'est souvent la pratique ou le calcul des nombres exprimés en chiffres qui a fait trouver, par induction, de belles propriétés des nombres dont la démonstration a exigé quelquefois une longue suite de propositions.

On a reconnu qu'il était utile de généraliser un peu la signification du mot *nombre* et l'on a désigné par ce mot un terme quelconque de la progression arithmétique dont la raison est 1, cette progression étant prolongée indéfiniment dans les deux sens, comme on le voit ci-dessous :

$$\ldots -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ldots.$$

Ainsi par le mot *nombre* on entendra 1° zéro; 2° l'unité positive et l'unité négative; 3° les nombres positifs et les nombres négatifs.

Pour l'intelligence de diverses propriétés des nombres, qui seront énoncées plus bas, afin de donner une idée de la théorie des nombres, il est bon de dire un mot de deux classifications des nombres. Il suffira de considérer les nombres positifs, les résultats étant les mêmes pour les nombres négatifs. Ces classifications d'un usage général se trouvent déjà dans les livres VII, VIII et IX des *OEuvres d'Euclide*. La première n'y est guère qu'indiquée.

Si l'on range la suite des nombres 0, 1, 2, 3, 4,..., des manières

suivantes :

$$\begin{cases} 0, 2, 4, 6,\ldots, \\ 1, 3, 5, 7,\ldots, \end{cases} \quad \begin{cases} 0, 3, 6,\ldots, \\ 1, 4, 7,\ldots, \\ 2, 5, 8,\ldots, \end{cases} \quad \begin{cases} 0, 4, 8, 12,\ldots, \\ 1, 5, 9, 13,\ldots, \\ 2, 6, 10, 14,\ldots, \\ 3, 7, 11, 15,\ldots, \end{cases}$$

on les distribuera d'abord en deux classes : 1° les nombres pairs renfermés dans la formule $2x$, puisque, en y posant $x = 0, 1, 2, 3,\ldots$, on retrouve $0, 2, 4, 6,\ldots$; 2° les nombres impairs renfermés dans la formule $2x + 1$. Autrement, la progression dont la raison est 1 a été partagée en deux autres dont la raison est 2.

On peut encore former trois classes, ou trois progressions dont la raison est 3, pour remplacer la progression dont la raison est 1 ; les nombres de ces trois classes sont représentés respectivement par

$$3x, \quad 3x + 1, \quad 3x + 2.$$

De même tous les nombres peuvent se partager en quatre classes, représentées par les formules

$$4x, \quad 4x + 1, \quad 4x + 2, \quad 4x + 3.$$

En général le nombre m étant pris à volonté, on formera m classes de nombres

$$mx, \quad mx + 1, \quad mx + 2,\ldots, \quad mx + m - 1.$$

Cette classification est importante, car on reconnaît bientôt que les propriétés des nombres varient selon qu'ils appartiennent à une classe ou à une autre.

2. On entend par *diviseur* d'un nombre n tout nombre qui s'y trouve contenu une ou plusieurs fois exactement; quel que soit n, les nombres 1 et n en sont diviseurs. Le nombre n est *premier* lorsqu'il n'a que ces deux diviseurs; il est *composé* dans le cas contraire. Les nombres 1, 2, 3, 5, 7, 11, 13, 17, 19,... sont premiers; ceux-ci, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20,... sont composés. Ainsi 4, outre les diviseurs 1 et 4, a le diviseur 2. Le nombre 9 a le diviseur 3, etc.

Un nombre composé est multiple de ses diviseurs : 12, qui a pour diviseur 4 ou qui contient 3 fois 4, est multiple de 4. Deux nombres sont *premiers entre eux* quand ils n'ont point d'autre diviseur *commun* que l'unité.

Les diviseurs de n, à l'exception de n, sont aussi nommés ***sous-multiples*** de n.

Les propriétés des nombres composés dépendent généralement de celles des nombres premiers dont ils sont multiples.

3. Ceci posé, voici quelques exemples de propriétés générales des nombres. Ils donneront une idée de ce qu'il faut entendre par Théorie des Nombres. Les applications montreront l'utilité de cette théorie pour le perfectionnement de certaines parties des mathématiques pures.

Premier exemple. — Euclide a prouvé qu'il y a une infinité de nombres premiers. Son raisonnement s'applique facilement aux nombres $4k+3$, mais cette proposition : *Il y a une infinité de nombres premiers de la forme* $4k+1$, est bien moins facile à établir que celle-ci : *Il y a une infinité de nombres premiers de la forme* $4k+3$.

Il est encore vrai de dire que toute progression arithmétique représentée par la formule

$$ax+r,$$

où r est premier à a, renferme une infinité de nombres premiers; mais la démonstration due à Lejeune-Dirichlet est assez compliquée.

Deuxième exemple. — Si l'on prend une progression arithmétique

$$5,\ 17,\ 29,\ 41,\ 53,\ 65,\ 77,\ 89,\ 101,\ 113,\ 125,\ 137,\ 149,\ \text{etc.},$$

et qu'on cherche les restes des termes divisés par un même nombre, on les verra se reproduire périodiquement. Pour le diviseur 7, la période de ces restes 5, 3, 1, 6, 4, 2, 0, est formée des sept termes 0, 1, 2, 3, 4, 5, 6.

Pour le diviseur 8 la période des restes 5, 1, est formée de deux termes. Généralement le nombre des termes de la période est égal au diviseur, ou à l'un de ses sous-multiples.

Troisième exemple. — Pour la progression geométrique, il y a quelque chose d'analogue. Soit, par exemple,

$$1,\ 5^1,\ 5^2,\ 5^3,\ 5^4,\ 5^5,\ 5^6,\ 5^7,\ldots,$$

ou

$$1,\ 5,\ 25,\ 125,\ 625,\ 3125,\ 15625,\ 78125,\ldots.$$

Si l'on prend pour diviseur le nombre premier 7, les restes sont

$$1,\quad 5,\quad 4,\quad 6,\quad 2,\quad 3,$$

et se reproduisent périodiquement.

Pour un autre diviseur premier, 13 par exemple, les quatre restes

$$1,\quad 5,\quad 12,\quad 8$$

se reproduisent périodiquement.

Généralement pour un diviseur premier p le nombre des termes de la période est un diviseur de $p-1$. On verra plus loin ce qui arrive quand le diviseur p n'est pas premier.

Cette proposition est intimement liée à la précédente, au moyen de la proposition suivante : *Le nombre a n'étant pas divisible par le nombre premier p, les restes des nombres*

$$a,\quad 2a,\quad 3a,\ldots,\quad (p-1)a,$$

divisés par p, sont, à l'ordre près,

$$1,\quad 2,\quad 3,\ldots,\quad p-1.$$

Exemple. Les nombres 5, 10, 15, 20, 25, 30, divisés par 7, donnent les restes 5, 3, 1, 6, 4, 2.

La proposition du troisième exemple revient à dire que si le nombre premier p ne divise pas a, le nombre $a^{p-1}-1$ est multiple de p. C'est le *Théorème de Fermat*. Euler l'a généralisé.

Quatrième exemple. — La décomposition des nombres en carrés donne la proposition suivante : *Il faut quatre carrés au plus pour former un nombre entier :*

$$2=1+1,\quad 3=1+1+1,\quad 4=1+1+1+1,\quad 5=4+1,$$
$$6=4+1+1,\quad 7=4+1+1+1,\quad 8=4+4,\ldots.$$

L'examen des formes particulières des nombres a conduit à des résultats remarquables, dont voici les énoncés :

Tout nombre premier $4k+1$ est la somme de deux carrés.

Tout nombre $8k+3$ est la somme de trois carrés.

Tout nombre impair est la somme de quatre carrés dont deux sont égaux, etc., etc.

Il faut cependant une étude assez approfondie des fonctions homo-

gènes du second degré $x^2 + y^2$, $x^2 + y^2 + z^2, \ldots$, pour avoir des démonstrations complètes.

On voit par cet exemple que l'analyse indéterminée, ou la résolution en nombres entiers des équations à plusieurs variables, conduit à des propriétés de nombres; malheureusement cette analyse est très-peu avancée au delà du second degré. Quant au premier degré, il ne présente pas de difficulté.

L'induction a indiqué certaines propositions qui n'ont pas encore été démontrées, peut-être parce qu'elles cessent d'être vraies au-delà d'une certaine limite. Selon Goldbach tout nombre pair est la somme de deux nombres premiers : $2 = 1 + 1$, $4 = 1 + 3$, $6 = 1 + 5$, etc. Il en résulterait que tout nombre impair est la somme de trois nombres premiers dont l'un serait l'unité.

4. La démonstration d'un théorème sur les nombres est dite *arithmétique* lorsqu'elle s'appuie uniquement sur la considération des nombres entiers et par suite des fractions, soit ordinaires, soit continues. Ces démonstrations méritent la préférence quand elles n'entraînent pas trop de longueur. Dans certains cas il faut, soit pour abréger considérablement, soit parce que l'on ne trouve aucune autre méthode, employer comme auxiliaires toute espèce de nombre : incommensurables, séries, intégrales définies, si le calcul donne le moyen de les faire disparaître du résultat final. Les expressions imaginaires facilitent assez souvent la démonstration de quelques théorèmes. Il en est même qu'on n'a pu encore établir sans leur secours. Ces démonstrations peuvent être nommées *analytiques;* elles seront quelquefois employées dans ce Traité, à défaut de plus simples purement arithmétiques.

CHAPITRE II.

DES NOMBRES COMPOSÉS. — PERMUTATIONS, NOMBRES FIGURÉS. — ARRANGEMENTS, COMBINAISONS. — PUISSANCE DU POLYNOME, DU BINOME. — NOMBRES POLYGONES.

8. On a remarqué que dans un produit de tant de facteurs qu'on voudra, on peut changer l'ordre des facteurs ; ainsi

$$2 \times 3 \times 4 = 2 \times 4 \times 3 = 24.$$

C'est une conséquence de ce que la multiplication n'est qu'un cas particulier de l'addition et que dans l'addition l'ordre des parties est indifférent. Mais pour le montrer bien clairement, il faut remarquer que si l'on convient de placer le multiplicateur à droite du multiplicande, on aura : 1° comme conséquence de l'addition

$$(a) \qquad (a+b+c+\ldots)m = am+bm+cm+\ldots;$$

2° comme conséquence directe de la définition

$$(b) \qquad a(m+n+p+\ldots) = am+an+ap+\ldots.$$

En langage ordinaire on peut dire :

Le multiple d'une somme est égal à la somme des multiples semblables des parties.

La somme de plusieurs multiples d'un nombre est un multiple de ce nombre.

Aux formules (a) et (b) il faut joindre la formule

$$(c) \qquad \left\{ \begin{aligned} (a+b+c\ldots)(m+n+p\ldots) = am+bm+cm+\ldots \\ +an+bn+cn+\ldots \\ +ap+bp+cp+\ldots \end{aligned} \right.$$

qui s'en déduit.

Il est à remarquer que les sommes $a+b+c+\ldots$, $m+n+p+\ldots$ ayant respectivement α et β termes, le produit en aura $\alpha\beta$. Donc : *Quand on prend un terme de la suite des nombres a, b, c,..., tous différents, avec un terme de la suite m, n, p,..., nombres aussi tous différents, cela se fait de $\alpha\beta$ manières.*

Ces propositions s'étendent à plus de deux sommes, à plus de deux suites de nombres.

La proposition suivante est une conséquence très-simple des formules (a) et (b).

THÉORÈME. — *Tout produit abcde... de plusieurs facteurs a, b, c, d, e,..., est multiple de chacun de ces facteurs et sa valeur ne change pas avec l'ordre des facteurs ou des multiplications successives. Chaque facteur est pris autant de fois qu'il y a d'unités dans le produit des autres facteurs.*

6. En représentant le produit $1.2.3\ldots n$ par Πn, on aura les propositions qui suivent :

THÉORÈME. — *Les m facteurs inégaux d'un produit peuvent être permutés de* Πm *manières.*

THÉORÈME. — *Si dans un produit de m facteurs il y en a $\alpha, \beta, \gamma,\ldots$, respectivement égaux à a, b, c,..., nombres différents, et que par conséquent on ait $\alpha+\beta+\gamma+\ldots=m$, le nombre des permutations sera*

$$\frac{\Pi m}{\Pi\alpha.\Pi\beta.\Pi\gamma\ldots}=\frac{\Pi(\alpha+\beta+\gamma+\ldots)}{\Pi\alpha.\Pi\beta.\Pi\gamma\ldots}.$$

Démonstration. — Admettons que parmi les facteurs il y en ait plusieurs égaux entre eux, les autres étant inégaux.

Pour fixer les idées, supposons trois facteurs égaux entre eux. La permutation

— a — b — c —

où les traits doivent être remplacés par des lettres de position invariable, en donne 2×3 par la permutation des lettres a, b, c; mais si l'on avait $a=b=c$, ces six se réduiraient à une seule.

On voit donc que toutes les permutations peuvent se partager en groupes de six termes analogues au précédent, car toutes les permutations d'un même groupe varient par la position de a, b, c.

Si les lettres a, b, c, viennent à changer et n'occupent plus les mêmes places, on a un nouveau groupe différent du précédent et renfermant aussi 2×3 permutations, et, comme il est impossible

de trouver un groupe renfermant moins de six permutations différentes, il faut conclure que le nombre des permutations, au lieu d'être Πm, sera $\frac{\Pi m}{2 \times 3}$. En général, si α facteurs sont égaux, on aura $\frac{\Pi m}{\Pi \alpha}$.

2° Si, indépendamment des α facteurs qui deviennent égaux, il y en a encore β qui le deviennent, un raisonnement tout semblable donnera $\frac{\Pi m}{\Pi\alpha . \Pi\beta}$, et ainsi de suite. On a donc ce résultat général :

$$\frac{\Pi m}{\Pi\alpha . \Pi\beta . \Pi\gamma \ldots} = \frac{\Pi(\alpha+\beta+\gamma+\ldots)}{\Pi\alpha . \Pi\beta . \Pi\gamma \ldots}.$$

Théorème. — *Le produit de* n *nombres consécutifs* $k+1$, $k+2, \ldots, k+n$ *est divisible par le produit* $1.2.3\ldots n = \Pi n$.

Démonstration. — Cela suit de ce que l'entier

$$\frac{\Pi(n+k)}{\Pi n . \Pi k} = \frac{\Pi k . (k+1)(k+2)\ldots(k+n)}{\Pi k . \Pi n}$$

se réduit à

$$\frac{(k+1)(k+2)\ldots(k+n)}{1 \;.\; 2 \;\ldots\; n}.$$

Cela vient encore des propositions suivantes, dont la vérité se voit immédiatement :

Théorème. — *La différence*

$$\frac{(k+1)(k+2)\ldots(k+n+1)}{1 \;.\; 2 \;\ldots\; (n+1)} - \frac{k(k+1)\ldots(k+n)}{1 \;.\; 2 \;\ldots (n+1)}$$

est égale à

$$\frac{(k+1)(k+2)\ldots(k+n)}{1 \;.\; 2 \;\ldots\; n}.$$

Théorème. — *La somme suivante*

$$\frac{1.2.3\ldots n}{1.2.3\ldots n} + \frac{2.3\ldots(n+1)}{1.2\ldots n} + \frac{3.4\ldots(n+2)}{1.2\ldots n} + \ldots + \frac{(k+1)(k+2)\ldots(k+n)}{1 \;.\; 2 \;\ldots\; n}$$

est égale à

$$\frac{(k+1)(k+2)\ldots(k+n+1)}{1 \;.\; 2 \;\ldots\; (n+1)}$$

qui se tire du dernier terme de la somme en mettant un facteur de plus au numérateur et au dénominateur.

Démonstration. — Si dans l'équation

$$\frac{(k+1)(k+2)\ldots(k+n+1)}{1.2\ldots(n+1)} - \frac{k(k+1)\ldots(k+n)}{1.2\ldots(n+1)} = \frac{(k+1)(k+2)\ldots(k+n)}{1.2\ldots n}$$

on fait $k = 1, 2, 3, \ldots$, et que l'on ajoute les équations ainsi obtenues membre à membre, en effaçant les termes qui se détruisent et transposant le terme $\frac{1.2\ldots(n+1)}{1.2\ldots(n+1)} = \frac{1.2\ldots n}{1.2\ldots n}$, on a le résultat de l'énoncé.

Des nombres figurés.

7. Les nombres représentés par la formule

$$\frac{x(x+1)(x+2)\ldots(x+n-1)}{1.2.3\ldots n}$$

sont dits *nombres figurés de l'ordre n*. Pour $n = 1$ on a les nombres *naturels*, pour $n = 2$ les nombres *triangulaires*, pour $n = 3$ les nombres *pyramidaux*, pour $n = 4$ les nombres *triangulo-triangulaires*, etc.

On peut les obtenir par des sommations successives, comme le montre le théorème du numéro précédent, qui peut se résumer ainsi :

$$\Sigma \frac{x(x+1)\ldots(x+n-1)}{1.2\ldots n} = \frac{x(x+1)\ldots(x+n)}{1.2\ldots(n+1)},$$

la somme Σ est composée de x termes qui répondent à

$$x = 1, 2, 3, \ldots, x.$$

Cette formule peut encore se présenter ainsi, pour éviter la forme fractionnaire,

$$(n+1)\Sigma x(x+1)\ldots(x+n-1) = x(x+1)\ldots(x+n).$$

Le tableau (a) qui suit, donne les nombres figurés des divers

ordres et leurs termes généraux,

$$(a)\quad \left\{\begin{array}{lllll} 1, & 1, & 1, & 1,\ldots, & 1, \\ 1, & 2, & 3, & 4,\ldots, & m, \\ 1, & 3, & 6, & 10,\ldots, & \dfrac{m(m+1)}{1.2}, \\ 1, & 4, & 10, & 20,\ldots, & \dfrac{m(m+1)(m+2)}{1.2.3}, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}\right.$$

où les termes généraux résultent des formules suivantes

$$\Sigma m = \frac{m(m+1)}{1.2} = 1+2+3+\ldots+m,$$

$$\Sigma\frac{m(m+1)}{1.2} = \frac{m(m+1)(m+2)}{1.2.3} = \frac{1.2}{1.2}+\frac{2.3}{1.2}+\frac{3.4}{1.2}+\cdots\frac{m(m+1)}{1.2},$$

$$\Sigma\frac{m(m+1)(m+2)}{1.2.3} = \frac{m(m+1)(m+2)(m+3)}{1.2.3.4} = \frac{1.2.3}{1.2.3}+\frac{2.3.4}{1.2.3}$$

$$+\frac{3.4.5}{1.2.3}+\cdots+\frac{m(m+1)(m+2)}{1.2.3}.$$

....

Fermat dans ses Notes sur *Diophante*, proposition IX du livre des *Polygones*, s'exprime ainsi :

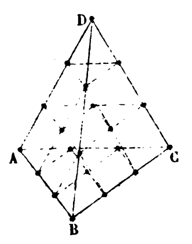
Propositionem pulcherrimam et mirabilem quam nos invenimus hoc in loco sine demonstratione apponemus. In progressione naturali quæ ab unitate sumit exordium quilibet numerus in proxime majorem facit duplum sui trianguli, in triangulum proxime majoris facit triplum suæ pyramidis, in pyramidem proxime majoris facit quadruplum sui triangulotrianguli, et sic uniformi et generali in infinitum methodo. Nec existimo pulchrius aut generalius in numeris posse dari theorema cujus demonstrationem margini inserere nec curat nec vacat.

Dans le tableau (a) la seconde ligne renferme les nombres naturels.

La troisième ligne les nombres dits triangulaires. Le nombre triangulaire de m est $\frac{m(m+1)}{1.2}$, son double est $m(m+1)$, produit de

$m + 1$ par m.

La quatrième ligne renferme les nombres pyramidaux. Le nombre pyramidal de m est $\frac{m(m+1)(m+2)}{1.2.3}$, son triple est $m\frac{(m+1)(m+2)}{1.2}$ ou le produit du nombre triangulaire de $m+1$ par m.



Dans ces figures, chaque point représente une unité. Ces points sont placés à égales distances sur les côtés d'un triangle équilatéral et sur des parallèles à la base de ce triangle.

Dans la figure qui représente le nombre pyramidal, les points sont placés sur des sections triangulaires équidistantes, faites parallèlement à la base d'un tétraèdre régulier.

La cinquième ligne du tableau (a) renferme les nombres triangulo-triangulaires. Ce nombre relativement à m est $\frac{m(m+1)(m+2)(m+3)}{1.2.3.4}$ dont le quadruple est $m.\frac{(m+1)(m+2)(m+3)}{1.2.3}$, produit du nombre pyramidal de $m+1$ par m, et ainsi de suite : c'est la règle de Fermat.

De son temps, les notations incommodes voilaient les conséquences même assez immédiates des opérations. Voici encore une démonstration élémentaire des équations

$$2\Sigma x = x(x+1),$$

$$3\Sigma x(x+1) = x(x+1)(x+2),$$

$$4\Sigma x(x+1)(x+2) = x(x+1)(x+2)(x+3),$$

. . . .

$$m\Sigma x(x+1)(x+2)\ldots(x+m-2) = x(x+1)(x+2)\ldots(x+m-1).$$

D'abord elles se vérifient pour $x = 1$, car en réduisant les sommes à un terme, l'équation générale donne

$$m.1.2.3...\overline{m-1} = 1.2.3...m.$$

Ensuite, si l'on suppose que l'équation est vraie jusqu'à une certaine valeur de x, en ajoutant un terme de plus, c'est-à-dire

$$m(x+1)(x+2)...(x+m-1),$$

le premier membre devient

$$m\Sigma(x+1)...(x+m-1),$$

et le second, par l'addition du même nombre, et en raison des facteurs communs,

$$(x+1)(x+2)...(x+m-1)(x+m);$$

ainsi il suffit de changer x en $x+1$ dans les deux membres et l'équation subsiste.

Cette méthode de démonstration, dite *de proche en proche*, est souvent employée comme moyen de vérification. Ainsi

$$\Sigma x^2 = \frac{x(x+1)(2x+1)}{1.2.3},$$

vraie pour $x = 1$, l'est en général, comme on le voit en ajoutant $(x+1)^2$ au premier membre et $(x+1)(x+1)$ au second. On a de même

$$\Sigma x^3 = \left[\frac{x(x+1)}{2}\right]^2.$$

Arrangements et combinaisons.

8. Dans l'arrangement des lettres $a, b, c, \ldots, l$, l'ordre peut être quelconque; dans la combinaison, on prend l'ordre alphabétique. Quand une même lettre peut être prise plusieurs fois, l'arrangement et la combinaison sont dits *avec répétition*. La formule qui donne la somme des nombres figurés conduit directement au nombre des combinaisons sans répétition ou avec répétition.

THÉORÈME. — *La formule qui donne le nombre $C_{m,n}$ des combinaisons, sans répétition, de m lettres n à n est*

$$C_{m,n} = \frac{m(m-1)(m-2)...(m-n+1)}{1.2.3..n}.$$

Théorème. — *La formule qui donne le nombre $C'_{m,n}$ des combinaisons, avec répétition, de m lettres n à n est*

$$C'_{m,n} = \frac{m(m+1)(m+2)\ldots(m+n-1)}{1.2.3\ldots n}.$$

Remarque. — Quand le nombre m des lettres est inférieur à n, la répétition est forcée; quand m égale n ou surpasse n, le nombre $C'_{m,n}$ s'étend aux combinaisons avec répétition et à celles sans répétition : c'est une conséquence de la manière dont on les forme et qui conduit immédiatement aux valeurs précédentes de $C_{m,n}$ et $C'_{m,n}$.

Démonstrations. — Soient les lettres $a, b, c, \ldots, l$ au nombre de m. Pour former les combinaisons deux à deux sans répétition, on placera a devant $b, c, \ldots, l$, ce qui donnera $m-1$ combinaisons. En plaçant b devant $c, d, \ldots, l$, on en aura $m-2$, et ainsi de suite, de sorte que l'on aura

$$C_{m,2} = (m-1)+(m-2)+\ldots+2+1 = \frac{m(m-1)}{1.2}.$$

Si les combinaisons étaient avec répétition, il faudrait placer a devant $a, b, c, \ldots, l$, et ainsi de suite, de sorte qu'on aurait

$$C'_{m,2} = m+(m-1)+\ldots+2+1 = \frac{m(m+1)}{1.2}.$$

Passant des combinaisons deux à deux aux combinaisons trois à trois, on aura semblablement, en plaçant a devant les combinaisons deux à deux des $m-1$ lettres $b, c, \ldots, l$, en plaçant b devant les combinaisons deux à deux des $m-2$ lettres $c, d, \ldots, l$, etc.,

$$C_{m,3} = \frac{(m-2)(m-1)}{1.2} + \frac{(m-3)(m-2)}{1.2} + \ldots + \frac{1.2}{1.2}$$
$$= \frac{(m-2)(m-1)m}{1.2.3},$$

et de même

$$C'_{m,3} = \frac{m(m+1)}{1.2} + \frac{(m-1).m}{1.2} + \ldots + \frac{1.2}{1.2} = \frac{m(m+1)(m+2)}{1.2.3},$$

et ainsi de suite : c'est précisément la sommation des nombres figurés.

Théorème. — *Le nombre des arrangements de m lettres n à n sans répétition est égal à m $(m-1)(m-2)\ldots(m-n+1)\ldots$ Par suite, le nombre des combinaisons de m lettres n à n sans répétition est*

égal au nombre des arrangements de m lettres n à n divisé par le nombre de permutations de n lettres.

THÉORÈME. — *Le nombre des arrangements de m lettres n à n avec répétition est égal au produit* $m.m\ldots\times m = m^n$.

Démonstration. — Cela suit de ce que les lettres $a, b, c, \ldots, l$ étant au nombre de m la puissance $(a+b+c+\ldots+l)^n$ sera composée de n^m termes, qui sont précisément les arrangements n à n avec répétition.

Puissances du polynôme et du binôme.

9. THÉORÈME. — *La puissance $n^{ième}$ du polynôme $a+b+c+\ldots+l$, formé de m termes, est donnée par la formule suivante :*

$$(a)\qquad (a+b+c+\ldots+l)^n = \Sigma.\frac{\Pi(\alpha+\beta+\gamma+\ldots)}{\Pi\alpha.\Pi\beta.\Pi\gamma\ldots}\,a^\alpha b^\beta c^\gamma\ldots,$$

où

$$\alpha+\beta+\gamma+\ldots = n,$$

ou bien

$$(b)\qquad \frac{(a+b+c+\ldots+l)^n}{\Pi(n)} = \Sigma.\frac{a^\alpha}{\Pi\alpha}.\frac{b^\beta}{\Pi\beta}.\frac{c^\gamma}{\Pi\gamma}\cdots.$$

Démonstration. — Les $n-1$ multiplications, qui donnent

$$(a+b+c+\ldots+l)^n,$$

produisent m^n termes : ce sont les arrangements de m lettres n à n *avec répétition.* Quand on rétablit l'ordre alphabétique, tous les termes qui donnent la même combinaison $a^\alpha b^\beta c^\gamma\ldots$ sont au nombre de $\frac{\Pi(\alpha+\beta+\gamma+\ldots)}{\Pi\alpha.\Pi\beta.\Pi\gamma\ldots}$, et l'on a la formule de l'énoncé.

THÉORÈME. — *Le nombre des termes du développement* $(a+b+c\ldots+l)^n$, *le nombre des lettres a, b, c,... l étant m, est égal à*

$$C'_{m,n} = \frac{m.(m+1)\ldots(m+n-1)}{1.2\ldots n}.$$

Démonstration. — Car, en supprimant les coefficients, on a les combinaisons de m lettres n à n avec répétition.

10. Pour le cas de deux lettres ou du binôme, on a $C_{2,m} = m+1$, et en effet les combinaisons avec répétition sont

$$a^m,\quad a^{m-1}b,\quad a^{m-2}b^2,\ldots,\quad a^1 b^{m-1},\quad b^m.$$

Dans ce cas on a la formule suivante :

THÉORÈME.

$$(a+b)^m = a^m + \frac{m}{1}a^{m-1}b + \frac{m(m-1)}{1.2}a^{m-2}b^2 + \ldots$$
$$+ \frac{m(m-1)\ldots(m-i+1)}{1.2\ldots i}a^{m-i}b^i + \ldots$$
$$+ \frac{m.m-1}{1.2}a^2b^{m-2} + \frac{m}{1}ab^{m-1} + b^m.$$

Démonstration. — Le coefficient de $a^\alpha b^\beta$, où $\alpha+\beta=m$, est

$$\frac{1.2.3\ldots(\alpha+\beta)}{1.2\ldots\alpha\times 1.2\ldots\beta}.$$

Par la suppression des facteurs communs aux deux termes il devient

$$\frac{(\alpha+1)(\alpha+2)\ldots(\alpha+\beta)}{1.2\ldots\beta} \quad\text{ou}\quad \frac{(\beta+1)(\beta+2)\ldots(\beta+\alpha)}{1.2\ldots\alpha},$$

ou encore, en posant $\beta = i$, d'où l'on tire $\alpha = m-i$,

$$\frac{m(m-1)\ldots(m-i+1)}{1.2\ldots i} \quad\text{ou}\quad \frac{m(m-1)\ldots(i+1)}{1.2\ldots m-i}.$$

Le coefficient $\frac{m(m-1)\ldots(m-i+1)}{1.2\ldots i}$ exprime donc de combien de manières on peut permuter m lettres composées de deux groupes, l'un de i mêmes lettres, l'autre de $m-i$ lettres aussi les mêmes.

Mais il a encore, comme on l'a vu, d'autres significations.

Voici des cas particuliers :

$$(a+b)^0 = 1,$$
$$(a+b)^1 = a+b,$$
$$(a+b)^2 = a^2+2ab+b^2,$$
$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3,$$
$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4,$$
$$(a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5,$$
$$(a+b)^6 = a^6+6a^5b+15a^4b^2+20a^3b^3+15a^2b^4+6ab^5+b^6.$$

. . . .

11. Les théorèmes qui suivent, montrent comment les nombres de combinaisons avec et sans répétition s'introduisent comme coefficients dans la formule du binôme.

THÉORÈME. — *Dans le produit* $(1 + ax)(1 + bx)\ldots(1 + lx)$, *les facteurs étant au nombre de* m, *le coefficient de* x^n *est la somme des combinaisons* n *à* n *des* m *lettres* $a, b, \ldots, l$. *Pour* $a = b = \ldots = l = 1$ *le produit devient* $(1 + x)^m$ *et le coefficient de* x^n *est*

$$C_{m,n} = \frac{m(m-1)\ldots(m-n+1)}{1.2\ldots n}.$$

THÉORÈME. — *Dans le produit de* m *facteurs*

$$(1 + ax + a^2x^2 + \ldots)(1 + bx + b^2x^2 + \ldots)\ldots(1 + lx + l^2x^2 + \ldots),$$

le coefficient de x^n *est la somme des combinaisons des* m *lettres* $a, b\ldots l$ *prises* n *à* n *avec et sans répétition.*

THÉORÈME. — *L'identité, après développement, de l'équation*

$$1 - a^k x^k = (1 - ax)(1 + ax + a^2x^2 + \ldots + a^{k-1}x^{k-1})$$

donne, pour $ax < 1$ *et* k *infini,*

$$\frac{1}{1 - ax} = 1 + ax + a^2x^2 + a^3x^3 + \ldots.$$

THÉORÈME. — *Dans l'hypothèse de* $x < 1$, *le développement de*

$$\frac{1}{(1 - ax)(1 - bx)\ldots(1 - lx)}$$

$$= (1 + ax + a^2x^2 + \ldots)(1 + bx + b^2x^2\ldots)\ldots(1 + lx + l^2x^2 + \ldots)$$

a pour coefficient de x^n *la somme des combinaisons* n *à* n *avec et sans répétition des* m *lettres* $a, b, \ldots, l$.

Pour $a = b = \ldots = l = 1$, *le développement de* $\frac{1}{(1-x)^m} = (1 - x)^{-m}$ *a pour coefficient de* x^n *le nombre* $C'_{m,n} = \frac{m(m+1)\ldots(m+n-1)}{1.2\ldots n}$.

Remarque. — Le développement de $(1 - x)^m$ étant

$$1 - mx + \frac{m(m-1)}{1.2}x^2 - \frac{m(m-1)(m-2)}{1.2.3}x^3 + \ldots,$$

le changement de m en $-m$ donnera

$$(1 - x)^{-m} = 1 + \frac{m}{1}x + \frac{m(m+1)}{1.2}x^2 + \ldots + C'_{m,n}x^n + \ldots,$$

comme dans le théorème précédent. Généralement la formule du binôme, pour l'exposant entier, s'étend à un exposant quelconque.

12. Si en prenant pour point de départ la suite des nombres

$$a,\ b,\ b,\ b,\ b,\ b,\ b,\ b\ldots,$$

on opérait comme pour obtenir les nombres figurés, en partant de la suite

$$1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ldots,$$

on formerait le tableau suivant :

$$(c)\left\{\begin{array}{llllr} a, & b, & b, & b,\ldots, & b, \\ a, & a+b, & a+2b, & a+3b,\ldots, & a+(n-1)b, \\ a, & 2a+b, & 3a+3b, & 4a+6b,\ldots, & na+\dfrac{(n-1)n}{1.2}b, \\ a, & 3a+b, & 6a+4b, & 10a+10b,\ldots, & \dfrac{n(n+1)}{1.2}a+\dfrac{(n-1)n(n+1)}{1.2.3}b, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}\right.$$

où les sommations se ramènent à celles des nombres figurés.

La deuxième ligne est la progression arithmétique dont le premier terme est a et la raison b.

La troisième ligne donnerait pour $a=1$ les nombres polygones.

L'équation

$$a+(a+b)+(a+2b)+\ldots+[a+(n-1)b]=\frac{1}{2}n[2a+(n-1)b]$$

donne les solutions de divers problèmes et les démonstrations de divers théorèmes.

Pour $a=1$, $b=2$, on a

$$1+3+5+7+\ldots+2n-1=n^2;$$

cette équation fournit un moyen facile de former les carrés consécutifs.

Si dans la même hypothèse de $b=2$, qui change le second membre en

$$n(a+n-1),$$

on voulait trouver pour somme le cube n^3, il faudrait poser

$$a+n-1=n^2,$$

ce qui détermine le premier terme $a=n^2-n+1$.

Ainsi pour $n=7$, si avec 7 nombres impairs consécutifs on veut

former $7^3 = 49 \cdot 7 = 343$, il faut prendre pour premier terme

$$49 - 7 + 1 = 43;$$

en effet,

$$43 + 45 + 47 + 49 + 51 + 53 + 55 = 343.$$

Pour les questions de ce genre, qui ne présentent aucune difficulté, on peut consulter une article de M. Wheatstone; le résumé se trouve dans le tome V du *Cosmos*.

Nombres polygones.

13. Si dans le terme général de la troisième ligne du tableau (c) on fait $a = 1$, on aura

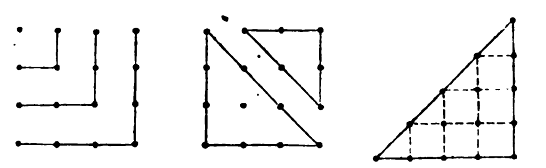
$$1 + (1+b) + (1 + 2b) + \ldots + [1 + b(n-1)] = n + b\,\frac{(n-1)n}{1.2},$$

ou bien encore

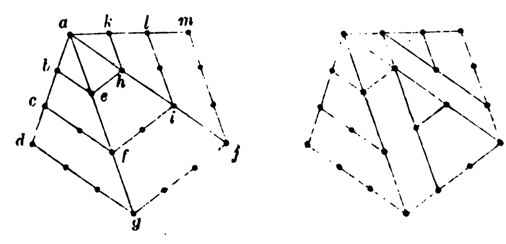
$$= \frac{n(n+1)}{1.2} + (b-1)\frac{(n-1)n}{1.2},$$

c'est là le nombre polygonal de $b+2$ côtés égaux à n; il est formé de b nombres triangulaires, l'un égal à $\frac{n(n+1)}{1.2}$ ou de côté n, et $b-1$ égaux à $\frac{(n-1)n}{1.2}$ ou de côté $n-1$.

Pour $b = 1, 2, 3, 4, \ldots$, on a les nombres triangulaires, carrés, pentagone, hexagone, etc., représentés par les figures suivantes :



Ces figures montrent la double décomposition en triangles et en termes consécutifs de la progression d'où l'on tire les nombres polygones.



On trouve, dans les Notes de Fermat sur le commentaire des Livres arithmétiques de *Diophante* par Bachet, cette remarque intéressante, à la suite d'une Note sur la décomposition des nombres en carrés :

Imo propositionem pulcherrimam et maxime generalem nos primi deteximus. Nempe omnem numerum vel esse triangulum, vel ex duobus aut tribus triangulis compositum; esse quadratum vel aut duobus aut tribus aut quator quadratis compositum; esse pentagonum aut ex duobus, tribus, quatuor aut quinque pentagonis compositum, et sic deinceps in infinitum in hexagonis, heptagonis et polygonis quibuslibet enuntianda, videlicet pro numero angulorum generali et mirabili; ejus autem demonstrationem quæ ex multis variis et abstrusissimis numerorum mysteriis derivatur hic apponere non licet, opus enim et librum integrum huic operi destinare decrevimus et arithmeticen hac in parte ultra veteres et notos terminos mirum in modum promovere.

La démonstration de Fermat n'est pas connue, Cauchy en a donné une très-remarquable en modifiant l'énoncé. La formule du polygone pour $n=1$ se réduit à 1 quel que soit b, pour $n=0$ elle se réduit à zéro, bien que zéro ne résulte pas des sommations indiquées. En regardant 0, 1 comme des polygones de $b+2$ côtés, on peut dire avec Cauchy que tout nombre peut se décomposer en m nombres polygones de m côtes, qui, à l'exception de quatre, sont 0 ou 1. Ce théorème est plus précis que celui de Fermat. On pourrait encore, comme le fait Legendre dans sa *Théorie des nombres*, modifier l'énoncé d'une autre manière.

Les nombres polygones, représentés par la formule

$$\left(1-\frac{b}{2}\right)x+\frac{b}{2}x^2,$$

ne sont qu'un cas particulier des nombres représentés par la formule

$$(a) \qquad a+bx+cx^2.$$

Quand on met dans cette formule, à la place de x, des nombres en progression arithmétique, par exemple :

$$0,\quad 1,\quad 2,\quad 3,\quad 4,\ldots,$$

ou plus généralement

$$\alpha, \quad \alpha+\beta, \quad \alpha+2\beta, \quad \alpha+3\beta, \ldots,$$

on obtient une suite de nombres dont les différences premières forment une progression arithmétique ordinaire ou de premier ordre, et dont les différences secondes (différences des différences) sont constantes. On dit que la formule (a) donne des nombres en progression arithmétique du second ordre.

CHAPITRE III.

DIVISEURS DES NOMBRES. — CARACTÈRES DE DIVISIBILITÉ. — RECHERCHE DU PLUS GRAND DIVISEUR COMMUN A DEUX OU PLUSIEURS NOMBRES. — RECHERCHE DU MOINDRE MULTIPLE DE PLUSIEURS NOMBRES. — PROPRIÉTÉ FONDAMENTALE DES NOMBRES PREMIERS ENTRE EUX. — RESTES DES NOMBRES EN PROGRESSION ARITHMÉTIQUE. — FRACTIONS CONTINUES.

14. Dans l'équation

$$a = bx + y,$$

où a et b sont des entiers donnés, x un entier variable pris à volonté, y sera nécessairement aussi entier positif, négatif ou nul. Dans tous les cas on dit que y est *résidu* de a pour le *module* b.

Dans l'équation souvent employée

$$a = mb + c,$$

où c tombe entre o et b, on dit que c est le résidu minimum positif de a pour le module b.

Pour l'équation

$$a = m'b - c',$$

où c' tombe entre o et b, on dit que $-c'$ est le résidu minimum négatif de a pour le module b; il est question de la valeur absolue.

Le résidu minimum positif étant c, comme l'équation

$$a = mb + c$$

revient à

$$a = (m+1)b - (b-c),$$

le résidu minimum négatif sera

$$-(b-c) = -c',$$

d'où l'on tire

$$c + c' = b,$$

on peut donc passer immédiatement de l'un des résidus à l'autre.

Comme des équations

$$a = mb + c, \quad a = (m+1)b - (b-c),$$

il résulte que l'on a

$$m < \frac{a}{b} < m+1,$$

on a coutume de représenter m par $E\left(\frac{a}{b}\right)$ pour dire l'entier de $\frac{a}{b}$. Quand a est multiple de b, on a $E\left(\frac{a}{b}\right) = \frac{a}{b}$.

Gauss et les auteurs allemands emploient le signe $\left[\frac{a}{b}\right]$.

Au moyen de ces notions, on reconnaît l'exactitude des propositions suivantes, qui résument la numération.

Théorème. — *Tout nombre positif* n *peut être mis sous la forme*

$$n = a + b\theta + c\theta^2 + d\theta^3 + \ldots + k\theta^m,$$

les nombres a, b, c,..., k étant positifs ou nuls et inférieurs à θ. Cette décomposition de n *est unique pour une même valeur de θ.*

Remarque I. — Si l'on convenait de prendre les nombres a, b, c,... non supérieurs à la moitié de θ, ils seraient les uns positifs, les autres négatifs, k seul serait toujours positif. La forme donnée à n serait encore unique; seulement, pour θ pair, il faudrait convenir de prendre $\frac{\theta}{2}$ avec le signe positif.

Remarque II. — Pour $\theta = 10$ on a l'expression de n dans le système décimal; a, b, c,... sont les chiffres du nombre. Si $\theta = 10^2$, on voit tout de suite que a, b, c,... sont des *tranches* de deux chiffres, et généralement des tranches de m chiffres, si $\theta = 10^m$.

Comme $\theta^m - 1$ est divisible par $\theta - 1$, et que de même $\theta^{2m} - 1$, $\theta^{2m+1} + 1$ sont divisibles par $\theta + 1$, on déduit de l'équation

$$n = k\theta^m + i\theta^{m-1} + \ldots + c\theta^2 + b\theta + a,$$

des règles simples pour reconnaître si de petits nombres, tels que 2, 3, 5, 7, 11, 13, divisent n.

Pour $\theta = 10$, n est exprimé dans le système décimal, et comme $\theta = 10 = 2 \times 5$, pour que n soit divisible par 2 ou 5, il faut et il suffit que a le soit.

La valeur de n conduisant à

$$n = k(\theta^m - 1) + i(\theta^{m-1} - 1) + \ldots + c(\theta^2 - 1) + b(\theta - 1) + k + i + \ldots + c + b + a,$$

ou

$$n = (\theta - 1)q + (a + b + c \ldots + i + k),$$

la divisibilité de n, par $\theta - 1$, ou un diviseur de $\theta - 1$ a pour condition nécessaire et suffisante que $a + b + \ldots + i + k$, somme des chiffres, soit divisible par $\theta - 1$ ou par le diviseur de $\theta - 1$, on a ainsi les règles pour 3, 9.

L'expression

$$n = a - b + c - d + \ldots + b(\theta + 1) + c(\theta^2 - 1) + d(\theta^3 + 1) \ldots,$$

ou

$$n = a - b + c - d \ldots + (\theta + 1)q,$$

donne la règle pour la divisibilité par $\theta + 1$ ou l'un de ses diviseurs, pour $\theta = 10$ on a la règle pour reconnaître si 11 divise un nombre.

Si l'on prend pour θ une puissance de 10, par exemple 10^3, on trouvera des règles de divisibilité par les diviseurs de $10^3 - 1$ et $10^3 + 1$. Comme $10^3 + 1 = 1001 = 7.11.13$, on a une règle assez simple pour reconnaître si un nombre est divisible par 7, 11 ou 13.

Soit le nombre 32788. On la partagera en tranches de trois chiffres, on prendra $788 - 32 = 756$; or 756 est divisible par 7, et ne l'est ni par 11, ni par 13; d'où il résulte que des trois nombres 7, 11, 13, il n'y a que 7 qui divise 32788.

L'emploi des Tables est bien préférable, mais il ne s'étend facilement qu'aux nombres inférieurs à une certaine limite.

Recherche du plus grand commun diviseur de deux ou de plusieurs nombres.

18. Le plus grand nombre qui divise chacun des nombres a, b, sera représenté par $D(a, b)$, et généralement $D(a, b, c, \ldots)$ indiquera le plus grand nombre qui divise chacun des nombres $a, b, c, \ldots$. La détermination du nombre $D(a, b, c, \ldots)$ dépend des propositions suivantes, données par Euclide dans le VII[e] livre de ses *Éléments*.

Théorème. — *Formez la suite d'entiers décroissants $a, b, c, d, \ldots$, tels que de trois nombres consécutifs le troisième soit le résidu mi-*

nimum positif du premier, le second étant pris pour module; la suite se terminera par les deux nombres k et o, *et k sera le nombre* $D(a, b) = D(b, c) = D(c, d) = \ldots = D(h, i) = D(i, k) = k$.

Démonstration. — On a

$$(a) \quad \begin{cases} a = ba' + c, & b = cb' + d, \quad c = dc' + e, \ldots, \\ f = gf' + h, & g = hg' + i, \quad h = ih' + k, \quad i = ki'. \end{cases}$$

Comme les restes $c, d, e, \ldots,$ vont en décroissant, il est nécessaire que la suite s'arrête.

Cette remarque déjà faite, que la somme de deux multiples d'un nombre est un multiple de ce nombre, qu'il en est de même de la différence de deux multiples d'un nombre, et enfin que tout multiple d'un multiple d'un nombre est multiple de ce nombre, montre que l'équation

$$a = bq \pm c$$

conduit à

$$D(a, b) = D(b, c).$$

D'après cette remarque, les équations données plus haut entraînent $D(a,b) = D(b,c) = \ldots = D(f, g) = D(g,h) = D(h,i) = D(i,k) = k$.

Voici des conséquences des équations (a) qui donnent le plus grand commun diviseur des nombres a, b.

Théorème. — *Tout diviseur commun de* a *et* b *est aussi diviseur de* D(a, b).

Théorème. — *On a*

$$D(a, b, c) = D[D(a, b), c] = D[D(a, c), b] = D[D(b, c), a].$$

Ces formules, dont l'exactitude s'établit en quelques mots, font voir que l'ordre des nombres $a, b, c, \ldots$ peut varier sans que le résultat change.

Théorème. — *On a*

$$D(a, b, c, d) = D[D(a, b, c), d] = \ldots,$$
$$D(a, b, c, d) = D[D(a, b), D(c, d)] = \ldots$$

Ces formules s'étendent à tant de nombres qu'on voudra.

Théorème. — *Tout nombre qui divise chacun des nombres* $a, b, c, d, \ldots$ *divise aussi* $D(a, b, c, d, \ldots)$.

Remarque. — Comme le nombre k divise les nombres $i, h, \ldots c, b, a$, les équations (a) se simplifieront par la division. La supposition de a et b premiers entre eux donne le système

$$a = ba' + c, \quad b = cb' + d, \quad c = dc' + e, \ldots$$
$$f = gf' + h, \quad g = hg' + i, \quad h = ih' + 1,$$

d'où, par de simples éliminations et en remontant de la dernière à la première, on obtient la proposition suivante :

16. Théorème. — *De la suite des nombres*

$$a, \quad b, \quad c, \ldots, \quad h, \quad i, \quad k = \mathrm{D}(a, b)$$

on peut déduire une autre suite

$$a_1, \quad b_1, \quad c_1, \ldots, \quad h_1, \quad i_1,$$

ces nombres, respectivement inférieurs à

$$\frac{a}{\mathrm{D}(a, b)}, \quad \frac{b}{\mathrm{D}(a, b)}, \ldots, \quad \frac{h}{\mathrm{D}(a, b)}, \quad \frac{i}{\mathrm{D}(a, b)},$$

étant tels que les valeurs absolues des différences

$$ab_1 - ba_1, \quad bc_1 - cb_1, \ldots, \quad hi_1 - ih_1,$$

sont égales à $\mathrm{D}(a, b)$, *et par conséquent à l'unité, quand* a *et* b *sont premiers entre eux.*

Cette propriété est fondamentale, elle résulte d'une autre plus générale qui sera donnée plus loin.

Du moindre multiple de plusieurs nombres.

17. Le moindre multiple des nombres a et b sera représenté par $m(a, b)$, de même le moindre multiple des nombres $a, b, c, \ldots$ le sera par $m(a, b, c, \ldots)$. La recherche du moindre multiple se fait au moyen des propositions qui suivent :

Théorème. — *Pour que* ma *soit multiple de* b, *on doit avoir* m *multiple de* $\frac{b}{\mathrm{D}(a, b)}$. *Autrement,* $\frac{abz}{\mathrm{D}(a, b)}$ *est la formule des multiples de* a *et* b. *Le moindre multiple* $m(a, b)$ *égale* $\frac{ab}{\mathrm{D}(a, b)}$, *et l'on a*

$$ab = m(a, b) . \mathrm{D}(a, b).$$

Démonstration. — Prenons les équations

$$a = ba' + c, \quad b = cb' + d, \quad c = dc' + e, \quad d = ed',$$

d'où l'on tire

$$e = \mathrm{D}(a, b).$$

Comme $ma = mba' + mc$, on aura mc multiple de b. De même $mb = mcb' + md$ donne md multiple de b, et $mc = mdc' + me$ donne me ou $m\mathrm{D}(a, b)$ multiple de $b = b'.\mathrm{D}(ab)$, et par suite m multiple de b' ou de $\frac{b}{\mathrm{D}(ab)}$. Puisque $m = \frac{bz}{\mathrm{D}(a, b)}$, on aura

$$ma = \frac{abz}{\mathrm{D}(ab)}$$

pour tout multiple de a qui l'est aussi de b.

Le moindre multiple de a et b répond à $z = 1$, on a donc

$$m(a, b) = \frac{ab}{\mathrm{D}(a, b)},$$

ou bien encore

$$ab = m(a, b).\mathrm{D}(a, b).$$

Théorème. — *Tout multiple de a et b est multiple de m(a, b) ou du moindre multiple de a et b.*

Remarque. — Cette proposition s'étend à tant de nombres qu'on voudra.

Théorème. — *On a*

$$m(a, b, c) = m[m(a, b), c] = m[m(a, c), b] = m[m(b, c), a].$$

C'est-à-dire que, pour avoir le moindre multiple de trois nombres, on peut prendre le moindre multiple de deux d'entre eux, puis le moindre multiple de ce nombre et du troisième des nombres donnés.

Théorème. — *On a*

$$m(a, b, c, d) = m[m(a, b, c), d] = \ldots$$

et

$$m(a, b, c, d) = m[m(a, b), m(c, d)] = \ldots.$$

Dans ces formules et toutes celles du même genre qui se présentent immédiatement, l'ordre des nombres venant à changer, le résultat reste le même. Elles ne diffèrent des précédentes que par le changement de D en m.

Remarque. — La formule du moindre multiple pour tant de nombres qu'on voudra sera donnée dans le chapitre suivant, sous une forme analogue à celle de l'équation $m(a, b) = \frac{ab}{D(a, b)}$, forme, il est vrai, sans application *pratique*, mais très-utile *en théorie*.

Simplification du calcul du nombre D(a, b).

18. On peut dans l'équation $a = ba' + c$ prendre indifféremment pour c le résidu minimum positif ou le résidu minimum négatif. Ainsi $29 = 6.4 + 5$ peut être remplacé par $29 = 6.5 - 1$. Pour la brièveté du calcul, il est bon de prendre celui des résidus qui a la moindre valeur absolue. Le calcul s'abrége quelquefois encore plus au moyen de la remarque suivante : le nombre k étant premier à a, on a $D(a, kb) = D(a, b)$, puisque tout diviseur de a qui divise kb divise b. D'après cela, on mettra en évidence dans c, quel que soit son signe, un facteur a'' premier à b, on remplacera c par $a''c$, c étant positif et a'' étant positif ou négatif selon le cas. L'équation $a = ba' + a''c$ donnera $D(a, b) = D(b, c)$. Dans cette équation a' sera un des entiers consécutifs entre lesquels tombe $\frac{a}{b}$. Pour $a' < \frac{a}{b}$, on pourra avoir $a' = 1$; quant à a'', il sera positif. Pour $a' > \frac{a}{b}$, on aura toujours $a' > 1$ et a'' sera négatif. On admettra donc le système

$$a = ba' + a''c, \quad b = cb' + b''d, \quad c = dc' + c''e, \ldots$$

qui donne aussi

$$D(a, b) = D(b, c) = D(c, d) = \ldots.$$

Ainsi pour deux nombres impairs a et b, en supposant a' impair, $a''c$ est pair et l'on prendra pour a'' la plus haute puissance de 2 qui divise $a - ba'$, cette puissance ayant le même signe que $a - ba'$.

19. Ceci expliqué, voici une conséquence importante du système d'équations qui donne $D(a, b)$. Pour simplifier, on peut réduire à six le nombre de ces équations ; la loi du calcul se manifeste de même.

Les équations

$$(1)\quad \left\{\begin{aligned} a &= ba' + a''c, \\ b &= cb' + b''d, \\ c &= dc' + c''e, \\ d &= ed' + d''f, \\ e &= fe' + e''g, \\ f &= gf'; \end{aligned}\right. \qquad (2)\quad \left\{\begin{aligned} a_1 &= b_1 a' + a'' c_1, \\ b_1 &= c_1 b' + b'' d_1, \\ c_1 &= d_1 c' + c'' e_1, \\ d_1 &= e_1 d' + d'' f_1, \\ e_1 &= f_1 e', \\ f_1 &= 1; \end{aligned}\right.$$

$$(3)\quad \left\{\begin{aligned} ab_1 - ba_1 &= a''(cb_1 - bc_1) = a''b''c''d''e''\,\mathrm{D}(a, b), \\ bc_1 - cb_1 &= b''(dc_1 - cd_1) = -\,b''c''d''e''\,\mathrm{D}(a, b), \\ cd_1 - dc_1 &= c''(ed_1 - de_1) = +\,c''d''e''\,\mathrm{D}(a, b), \\ de_1 - ed_1 &= d''(fe_1 - ef_1) = -\,d''e''\,\mathrm{D}(a, b), \\ ef_1 - fe_1 &= e''.\mathrm{D}(a, b), \end{aligned}\right.$$

se vérifient presque immédiatement. Les équations (2) ne diffèrent des équations (1) que par le changement de a, b, c, d en a_1, b_1, c_1, d_1, les deux dernières $e_1 = f_1 e'$, $f_1 = 1$ sont données à priori. L'élimination de a', b', c', d', entre les équations correspondantes (1) et (2) donne les deux premiers membres des équations (3), la dernière équation (3) n'est que l'avant-dernière du système (1). La multiplication membre à membre des équations (3) et la suppression des facteurs communs donnent les troisièmes membres.

On peut aussi trouver ces équations comme il suit :

La dernière équation du système (3) n'est autre que l'avant-dernière du système (1) $e = fe' + e''g$, puisque l'on a

$$g = \mathrm{D}(a, b), \quad f_1 = 1 \quad \text{et} \quad e_1 = e' = e'f_1.$$

L'avant-dernière équation du système (3) vient de l'équation

$$d = ed' + d''f$$

d'où l'on a éliminé f au moyen de l'équation

$$fe_1 = ef_1 - e''\mathrm{D}(a, b).$$

La réduction se fait en posant

$$d_1 = e_1 d' + d'' f_1.$$

L'antépénultième équation du système (3) se tire de même de l'équation

$$c = dc' + c''e$$

par l'élimination de e, en posant

$$c_1 = d_1c' + c''e_1,$$

et ainsi de suite. L'équation la plus importante est

$$ba_1 - ab_1 = -a''\,b''\,c''\,d''\,e''\,\mathrm{D}(a, b).$$

Si l'on prend $a'' = b'' = c'' = \ldots = 1$, comme dans la méthode ordinaire, on aura

$$ba_1 - ab_1 = (-1)^n\,\mathrm{D}\,(a, b),$$

n étant le nombre des termes de la suite $a'', b'', c'', d'', e'' \ldots$, ou le nombre des équations qui donnent $\mathrm{D}(a, b) = g$.

Si l'on prenait

$$a'' = b'' = c'' = \ldots = -1,$$

on aurait

$$ba_1 - ab_1 = \mathrm{D}(a, b).$$

Les équations (1) et (2) donnent

$$\frac{a}{g} - a_1 = a'\left(\frac{b}{g} - b_1\right) + a''\left(\frac{c}{g} - c_1\right),$$

$$\frac{b}{g} - b_1 = b'\left(\frac{c}{g} - c_1\right) + b''\left(\frac{d}{g} - d_1\right),$$

$$\frac{c}{g} - c_1 = c'\left(\frac{d}{g} - d_1\right) + c''\left(\frac{e}{g} - e_1\right),$$

$$\frac{d}{g} - d_1 = d'\left(\frac{e}{g} - e_1\right) + d''\left(\frac{f}{g} - f_1\right),$$

$$\frac{e}{g} - e_1 = e'\left(\frac{f}{g} - f_1\right) + e''.$$

Pour $a'', b'', c'', \ldots$ égaux à 1, on reconnaît tout de suite que les premiers membres sont positifs, comme composés de parties positives.

Il en est encore de même pour $a'', b'', c'', \ldots$, égaux à -1, parce que $a', b', c', \ldots$, valent 2 au moins.

On est donc conduit à l'équation

$$ba_1 - ab_1 = \pm\,\mathrm{D}\,(a, b),$$

en supposant $a_1 < \frac{a}{D(a, b)}$, $b_1 < \frac{b}{D(a, b)}$, de sorte que ab_1 et ba_1 sont inférieurs à $m(a, b)$.

Si l'on prenait

$$a_1 = \frac{a}{D(a, b)} - a'_1, \qquad b_1 = \frac{b}{D(a, b)} - b'_1,$$

on aurait

$$ab'_1 - ba'_1 = \pm D(a, b),$$

le signe du second membre restant le même.

Restes des nombres en progression arithmétique.

20. Théorème. — *Quand on divise les termes successifs d'une progression arithmétique dont la raison est* **a**, *par un même nombre* **b**, *les restes forment une période de* $\frac{b}{D(a, b)}$ *termes inégaux. Le reste zéro se présente toujours si* $D(a, b) = 1$, *mais si* $D(a, b)$ *surpasse* 1, *il faut que* $D(a, b)$ *divise le premier terme* c, *pour que le reste zéro se présente.*

Démonstration. — On suppose les termes de la progression donnés par la formule $ax + c$ en y posant successivement

$$x = 0, 1, 2, 3, \ldots,$$

de sorte que le premier terme est c et la raison a. Afin qu'un reste déjà obtenu en faisant $x = \alpha$ se présente de nouveau pour $x = \alpha + \beta$, il faut et il suffit qu'on ait $a\beta$ multiple de b, ou β multiple de $\frac{b}{D(a, b)}$. On voit par là qu'il y a $\frac{b}{D(a, b)}$ restes différents répondant à

$$x = 0, 1, 2, 3, \ldots, \frac{b}{D(a, b)} - 1.$$

Ainsi pour $D(a, b) = 1$, il y a b restes, savoir, à l'ordre près,

$$0, 1, 2, 3, \ldots, b - 1.$$

Quand $D(a, b)$ surpasse 1, il y a $\frac{b}{D(a, b)}$ restes, et si l'on pose

$$c = c' D(a, b) + c'',$$

ils sont compris dans la formule $D(a, b)z + c''$, en y faisant

$$z = 0, 1, 2, \ldots, \frac{b}{D(a, b)} - 1.$$

Le reste zéro ne peut se présenter que quand $c'' = 0$; on suppose c'' positif et inférieur à $D(a, b)$.

Résolution de l'équation $ax + c = by$.

21. Problème. — *Les nombres a et b étant premiers entre eux, trouver la moindre valeur de x qui rend $ax + 1$ divisible par b, et par suite celle qui rend $ax + c$ divisible par b.*

Solution. — En supposant a plus grand que b, les équations du plus grand commun diviseur conduisent à l'équation

$$b\alpha - a\beta = \pm 1.$$

Pour le signe supérieur on a

$$b\alpha = a\beta + 1,$$

et la valeur de β est inférieure à b.

Si l'on multiplie par c et que dans

$$b(c\alpha) = a(c\beta) + c,$$

on fasse

$$c\beta = b\gamma + \beta',$$

il s'ensuivra que $a\beta' + c$ sera divisible par b, β' étant inférieur à b.

Si l'on avait eu

$$b\alpha = a\beta - 1,$$

comme α et β sont respectivement moindres que a et b, on aurait posé

$$\alpha = a - \alpha', \quad \beta = b - \beta',$$

et la réduction aurait donné, en changeant les signes,

$$b\alpha' = a\beta' + 1,$$

comme dans le cas précédent.

La solution particulière $x = \alpha$, $y = \beta$ donnant

$$a\alpha + c = b\beta \quad \text{et} \quad a(x - \alpha) = b(y - \beta),$$

on en tire la solution générale

$$x = \alpha + bu, \quad y = \beta + au,$$

où u est un entier quelconque.

Exemple. — Soit proposé de trouver : 1° le plus grand commun diviseur des nombres 522 et 151 ; 2° la moindre valeur de x qui rend $151x + 1$ divisible par 522 ; 3° la moindre valeur de x qui rend $151x + 7$ divisible par 522.

Voici le procédé à suivre :

(a)	(a')	(a_1)
522		121
151	3	35
69	2	16
13	5	3
4	3	1
1	4	0
0		

Dans la colonne (a) mettez d'abord 522 et 151 ; la division donnera le quotient 3, que vous placerez dans la colonne (a'), à côté de 151, et le reste 69 que vous placerez sous 151. Puis opérez sur 151 et 69, comme vous avez fait sur 522 et 151. Continuez ainsi jusqu'à ce que vous ayez obtenu le reste 0. Le reste précédent est le diviseur commun maximum. Ici c'est 1, les nombres 522 et 151 sont premiers entre eux. [*Voyez* p. 36, équations (1) et (2)].

Quand les nombres donnés ne sont pas premiers entre eux, il est bon de diviser par $D(a, b)$ tous les nombres de la colonne (a) ce qui diminue les nombres de la colonne (a_1) qui généralement se trouvent comme il suit : Prenez pour les deux derniers termes de la colonne (a_1), les deux derniers de la colonne (a) et placez-les à côté des derniers termes de la colonne (a'). Pour avoir les termes précédents de la colonne (a_1), il suffit de multiplier chaque terme de la colonne (a') par le terme correspondant de la colonne (a_1) et d'ajouter au produit le terme immédiatement inférieur de la même colonne. D'après cela les deux derniers termes font connaître le précédent, celui-ci à son tour fait connaître celui qui le précède, et ainsi de suite. Si l'on considère les deux colonnes (a), (a_1) ou les deux suites

$$a,\ b,\ c,\ d,\ldots,\ a_1,\ b_1,\ c_1,\ d_1,\ldots,$$

on reconnaît que les différences

$$ab_1 - ba_1, \quad bc_1 - cb_1, \quad cd_1 - dc_1, \ldots$$

sont égales à ± 1 ou $\pm [D(a, b)]^2$, selon que l'on aura ou non divisé par $D(a, b)$ tous les termes de la colonne (a) avant de calculer ceux de la colonne (a_1); en effet, quand la division par $D(a, b)$ n'a pas été faite, les nombres $a, b, c, \ldots a_1, b_1, c_1, \ldots$ sont tous divisibles par $D(a, b)$, et l'on a

$$\frac{a}{D(a, b)} \cdot \frac{b_1}{D(a, b)} - \frac{b}{D(a, b)} \cdot \frac{a_1}{D(a, b)} = \pm 1.$$

La règle pour trouver le signe dépend du nombre des quotients ou des termes de la colonne (a'); ce nombre étant n, on aura l'équation fondamentale

$$\frac{a}{D(a, b)} \cdot \frac{b_1}{D(a, b)} - \frac{b}{D(a, b)} \cdot \frac{a_1}{D(a, b)} = (-1)^n,$$

qui pour a, b premiers entre eux, cas principal auquel on est toujours ramené, devient

$$ab_1 - ba_1 = (-1)^n.$$

Dans le présent exemple on a

$$522.35 - 151.121 = -1;$$

mais si l'on pose

$$35 = 151 - 116,$$
$$121 = 522 - 401,$$

on trouve

$$522.116 - 151.401 = 1.$$

On a donc

$$151.401 + 1$$

divisible par 522. Multipliant par 7, il vient

$$151.2807 + 7$$

divisible par 522. Si l'on ôte de 2807 cinq fois 522 ou 2610, il reste 197, et l'on a

$$151.197 + 7$$

divisible par 522.

Ayant trouvé l'équation

$$522.35 = 151.121 - 1$$

pour rendre $151x + c$ divisible par 522, on aurait pu multiplier par $-c$

$$522(-35c) = 151(-121c) + c,$$

puis chercher le multiple de 522 immédiatement supérieur à $121c$; la valeur cherchée de x qui rend $151x + c$ divisible par 522, aurait

été la différence du multiple de 522 et de $121c$. Pour $c=7$, on a

$$121.7=847,\quad 522\times 2=1044,\quad 1044-847=197,$$

valeur trouvée plus haut

$$151.197+7=522.57.$$

22. Voici un second mode de calcul qui consiste à descendre de la première des équations (1), page 36, aux suivantes :

On forme, au moyen des nombres $a', b', c', d', \ldots$, les deux suites $x_1, x_2, x_3\ldots, y_1, y_2, y_3\ldots$ par les équations (4) et (5); l'élimination de $b', c', \ldots$, entre les équations correspondantes de deux systèmes (4) et (5) donne le système (6), et les équations de la recherche du plus grand commun diviseur donnent les équations (7) par de simples éliminations.

$$(4)\quad \begin{cases} x_1=a', \\ x_2=b'x_1+a'', \\ x_3=c'x_2+b''x_1, \\ x_4=d'x_3+c''x_2, \\ x_5=e'x_4+d''x_3, \end{cases}$$

$$(5)\quad \begin{cases} y_1=1, \\ y_2=b'y_1, \\ y_3=c'y_2+b''y_1, \\ y_4=d'y_3+c''y_2, \\ y_5=e'y_4+d''y_3, \end{cases}$$

$$(6)\quad \begin{cases} x_1y_2-x_2y_1=-a'', \\ x_2y_3-x_3y_2=+a''b'', \\ x_3y_4-x_4y_3=-a''b''c'', \\ x_4y_5-x_5y_4=+a''b''c''d'', \end{cases}$$

$$(7)\quad \begin{cases} bx_1-ay_1=-a''c, \\ bx_2-ay_2=+a''b''d, \\ bx_3-ay_3=-a''b''c''e, \\ bx_4-ay_4=+a''b''c''d''f, \\ bx_5-ay_5=-a''b''c''d''e''g. \end{cases}$$

La première équation (7) n'est que

$$a=ba'+a''c \quad \text{ou} \quad ba'-a.1=-a''c,$$

d'apres les notations (4) et (5). L'équation

$$b = cb' + b''d,$$

mise sous la forme

$$ba'' - b'a''c = a''b''d,$$

donne la seconde équation (7) en remplaçant a'' par $x_2 - b'x_1$ et $-a''c$ par $bx_1 - ay_1$.

Quand les deux premières équations (7) ont été vérifiées, comme les trois premières donnent

$$b(x_3 - c'x_2 - b''x_1) - a(y_3 - c'y_2 - b''y_1) = a''b''(c - dc' - c''e) = 0,$$

la troisième équation est aussi vérifiée.

Fractions continues.

23. Les fractions continues conduisent plus directement à l'équation

$$ay_5 - bx_5 = a''b''c''d''e''\,\mathrm{D}(a, b).$$

En effet, les équations

$$a = ba' + a''c,$$
$$b = cb' + b''d,$$
$$c = dc' + c''e,$$
$$d = ed' + d''f,$$
$$e = fe' + e''g,$$
$$f = gf',$$

de la recherche du plus grand commun diviseur de a, b donnent

$$\frac{a}{b} = a' + \frac{a''c}{b} = a' + \frac{a''}{\left(\frac{b}{c}\right)},$$

$$\frac{b}{c} = b' + \frac{b''d}{c} = b' + \frac{b''}{\left(\frac{c}{d}\right)},$$

$$\frac{c}{d} = c' + \frac{c''e}{d} = c' + \frac{c''}{\left(\frac{d}{e}\right)},$$

$$\frac{d}{e} = d' + \frac{d''f}{e} = d' + \frac{d''}{\left(\frac{e}{f}\right)},$$

$$\frac{e}{f} = e' + \frac{e''g}{f} = e' + \frac{e''}{\left(\frac{f}{g}\right)},$$

$$\frac{f}{g} = f',$$

par suite

$$\frac{a}{b}=a'+\cfrac{a''}{b'+\cfrac{b''}{\left(\frac{c}{d}\right)}}=a'+\cfrac{a''}{b'+\cfrac{b''}{c'+\cfrac{c''}{\left(\frac{d}{e}\right)}}}$$

$$=a'+\cfrac{a''}{b'+\cfrac{b''}{c'+\cfrac{c''}{d'+\cfrac{d''}{\left(\frac{e}{f}\right)}}}}=a'+\cfrac{a''}{b'+\cfrac{b''}{c'+\cfrac{c''}{d'+\cfrac{d''}{e'+\cfrac{e''}{f'}}}}}.$$

C'est là ce qu'on nomme fraction *continue;* le plus souvent on prend $a''=b''=c''=\ldots=1$. On a dans ce cas les fractions continues ordinaires à termes positifs, telles que

$$a'+\cfrac{1}{b'+\cfrac{1}{c'+\cfrac{1}{d'+\ldots}}}.$$

En prenant $a''=b''=c''=\ldots=-1$, on aurait les fractions

$$a'-\cfrac{1}{b'-\cfrac{1}{c'-\cfrac{1}{d'-\ldots}}}=a'+\cfrac{1}{-b'+\cfrac{1}{c'-\cfrac{1}{d'-\ldots}}}$$

$$=a'+\cfrac{1}{-b'+\cfrac{1}{c'+\cfrac{1}{-d'+\ldots}}},$$

dans laquelle les dénominateurs b', c', d',.. sont alternativement négatifs et positifs. Ces fractions, qui se sont présentées à Gauss (*Réduction des formes*), sont quelquefois plus avantageuses que celles à termes tous positifs.

Les équations

$$\begin{aligned} x_1 &= a', & y_1 &= 1 \\ x_2 &= b'x_1 + a'', & y_2 &= b'y_1, \\ x_3 &= c'x_2 + b''x_1, & y_3 &= c'y_2 + b''y_1, \\ x_4 &= d'x_3 + c''x_2, & y_4 &= d'y_3 + c''y_2, \\ x_5 &= e'x_4 + d''x_3, & y_5 &= e'y_4 + d''y_3, \\ \frac{a}{D(a, b)} &= x_6 = f'x_5 + e''x_4, & \frac{b}{D(a, b)} &= y_6 = f'y_5 + e''y_4, \end{aligned}$$

donnent par élimination

$$\begin{aligned} x_2 y_1 - y_2 x_1 &= a'', \\ x_3 y_2 - y_3 x_2 &= - a''b'', \\ x_4 y_3 - y_4 x_3 &= a''b''c'', \\ x_5 y_4 - y_5 x_4 &= - a''b''c''d''e'', \\ \frac{ay_5}{D(a, b)} - \frac{bx_5}{D(a, b)} &= a''b''c''d''e''. \end{aligned}$$

Les deux suites

$$x_1, \quad x_2, \quad x_3, \ldots,$$
$$y_1, \quad y_2, \quad y_3, \ldots,$$

s'obtiennent en faisant

$$\frac{x_1}{y_1} = a', \quad \frac{x_2}{y_2} = a' + \frac{a''}{b'}, \quad \frac{x_3}{y_3} = a' + \cfrac{a''}{b' + \cfrac{b''}{c'}} \cdots$$

On passe de $\frac{x_2}{y_2}$ à $\frac{x_3}{y_3}$ en changeant b' en $b' + \frac{b''}{c'}$ dans $\frac{x_2}{y_2}$, de $\frac{x_3}{y_3}$ à $\frac{x_4}{y_4}$ en remplaçant c' par $c' + \frac{c''}{d'}$, et ainsi de suite.

Quand on fait $a'' = b'' = c'' = \ldots = 1$, ce qui est le cas des fractions continues ordinaires, les fractions partielles

$$a', \quad a' + \frac{1}{b'}, \quad a' + \cfrac{1}{b' + \cfrac{1}{c'}}, \ldots,$$

ou encore

$$\frac{x_1}{y_1}, \quad \frac{x_2}{y_2}, \quad \frac{x_3}{y_3}, \ldots,$$

sont alternativement plus petites et plus grandes que la fraction $\frac{a}{b}$.

dont elles approchent de plus en plus; on les nomme **fractions *convergentes;*** et aussi ***réduites,*** parce qu'elles sont irréductibles, comme le montrent les équations

$$x_1 y_2 - x_2 y_1 = \pm 1.$$

Dans la fraction

$$a' + \cfrac{1}{-b' + \cfrac{1}{c' + \cfrac{1}{-d' - \ldots}}},$$

à termes alternativement positifs et négatifs, les expressions

$$a', \quad a' + \frac{1}{-b'}, \quad a' + \cfrac{1}{-b' + \cfrac{1}{c'}},$$

sont toutes plus grandes que $\frac{a}{b}$, dont elles s'approchent de plus en plus. Ces fractions réduites en fraction ordinaires sont aussi irréductibles.

Pour réduire une quantité réelle quelconque x en fraction continue ordinaire, on représente par $E(x)$ l'entier immédiatement inférieur à x, et l'on pose

$$x = E(x) + \frac{1}{x'};$$

comme $\frac{1}{x'}$ doit être moindre que l'unité, il faudra que x' surpasse 1. On fera de même

$$x' = E(x') + \frac{1}{x''},$$

et ainsi de suite; ce qui donne

$$x = E(x) + \cfrac{1}{E(x') + \cfrac{1}{E(x'') + \ldots}}.$$

Cette opération peut se prolonger à l'infini.

En représentant par $E'(x)$ l'entier immédiatement supérieur à x, on aurait eu

$$x = E'(x) - \frac{1}{x'}, \quad x' = E'(x') - \frac{1}{x''}, \ldots,$$

et de là

$$x = \mathrm{E}'(x) - \cfrac{1}{\mathrm{E}'(x') - \cfrac{1}{\mathrm{E}'(x'') - \dots}}$$

$$x = \mathrm{E}'(x) + \cfrac{1}{-\mathrm{E}'(x') + \cfrac{1}{\mathrm{E}'(x'') + \cfrac{1}{-\mathrm{E}'(x''') + \dots}}}$$

Quand on applique cette méthode à la réduction en fraction continue des racines incommensurables d'une équation du second degré à coefficients entiers

$$az^2 + bz + c = 0,$$

on trouve une fraction continue périodique, qui sert pour la résolution des équations indéterminées de la forme

$$ax^2 + bxy + cy^2 = n.$$

Cette remarque sera développée.

CHAPITRE IV.

DES NOMBRES PREMIERS. — DE LA DÉCOMPOSITION DES NOMBRES EN FACTEURS PREMIERS. — THÉORÈMES ÉLÉMENTAIRES.

24. On trouve facilement les nombres premiers des premières centaines au moyen de la proposition suivante :

THÉORÈME. — *Les nombres inférieurs à un carré a^2, s'ils sont composés, ont un facteur premier inférieur à a.*

Au-dessous de $4 = 2^2$, qui est le moindre des nombres composés, les nombres 1, 2, 3 sont premiers.

Au-dessous de $9 = 3^2$, les nombres composés sont multiples de 2; l'exclusion des multiples de 2 montre qu'entre 4 et 9 les nombres 5 et 7 sont premiers.

De même entre $9 = 3^2$ et $25 = 5^2$, l'omission des multiples de 2 et de 3 donne les nombres premiers 11, 13, 17, 19, 23.

Entre 25 et $49 = 7^2$, l'omission des multiples de 2, 3, 5 donne les nombres premiers 29, 31, 37, 41, 43, 47.

Entre 49 et $121 = 11^2$, l'omission des multiples de 2, 3, 5, 7 donne les nombres premiers 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113.

Entre 121 et $169 = 13^2$, l'omission des multiples des nombres 2, 3, 5, 7, 11 donne les nombres premiers 127, 131, 137, 139, 149, 151, 157, 163, 167, et ainsi de suite.

On trouvera plus loin une Table pour la décomposition des nombres inférieurs à 10000 en facteurs premiers. On a pour la décomposition des nombres en facteurs premiers différentes Tables, la plus récente dépasse 6 millions, celle de Burckhardt va jusqu'à 3036000.

On a les propositions suivantes, où les majuscules représentent des nombres premiers différents et rangés par ordre de grandeur.

THÉORÈME. — *Tout nombre* n *peut être mis sous la forme*

$$n = A^\alpha B^\beta C^\gamma \ldots,$$

A, B, C, ... *étant des nombres premiers croissants.*

Pour $\alpha = 1$, $\beta = \gamma = \ldots = 0$, n qui se réduit à A est un nombre premier.

THÉORÈME. — *Il y a une infinité de nombres premiers.*

Démonstration. — Soient 2, 3, 5, 7, ..., P tous les nombres premiers jusqu'à P, il y en a encore de plus grands, car si le nombre $1 + 1.2.3, \ldots P$ n'était pas premier, il aurait un diviseur premier nécessairement plus grand que P. (*OEuvres d'Euclide*, livre IX.)

THÉORÈME. — *Tout nombre premier* A *qui divise* mB *divise* m.

C'est une conséquence de $D(A, B) = 1$. On peut aussi le prouver directement par les équations

$$B = Aq + r, \quad B = rq' + r', \quad B = r'q'' + r'', \ldots;$$

il suffit de remarquer que la suite $r, r', r'' \ldots$ doit finir par le reste 1, et que

$$mr, mr', mr'', \ldots, m$$

sont divisibles par A, parce que l'on a

$$mB = mAq + mr, \quad mB = mrq' + mr', \text{ etc.}$$

Le cas de $A > B$ se traite de même.

THÉORÈME. — *Tout nombre premier* P *qui divise un produit, divise un de ses facteurs.*

THÉORÈME. — *La décomposition d'un nombre en facteurs premiers sous la forme* $A^\alpha B^\beta C^\gamma \ldots$ *est unique.*

THÉORÈME. — *Toute puissance* n^k *décomposée en facteurs premiers a la forme* $A^{\alpha k} B^{\beta k} C^{\gamma k} \ldots$ *en posant* $n = A^\alpha B^\beta C^\gamma \ldots$

THÉORÈME. — *Les diviseurs de* $n = A^\alpha B^\beta C^\gamma \ldots$ *ont la forme* $A^{\alpha'} B^{\beta'} C^{\gamma'} \ldots$, *les nombres* $\alpha', \beta', \gamma', \ldots$ *étant au plus égaux aux nombres correspondants* $\alpha, \beta, \gamma \ldots$

$\alpha' = \beta' = \gamma' = \ldots = 0$ donne le diviseur 1.

$\alpha' = \alpha$, $\beta' = \beta$, $\gamma' = \gamma, \ldots$ donne le nombre n lui-même.

On nomme nombres *premiers entre eux* ceux qui n'ont aucun diviseur commun excepté 1. La décomposition en facteurs premiers rend évidentes les propositions suivantes.

THÉORÈME. — *Si les nombres $a, b, c, \ldots$ sont premiers à k, leur produit l'est aussi.*

THÉORÈME. — *Si les nombres $a, b, c, \ldots$, premiers entre eux deux à deux, divisent k, le produit $abc\ldots$ divisera aussi k.*

THÉORÈME. — *Si une puissance d'exposant k est décomposée en facteurs premiers entre eux deux à deux, ces facteurs seront des puissances d'exposant k.*

THÉORÈME. — *Les diviseurs de $n = A^a B^b C^c \ldots$ sont les termes du produit*

$$(1 + A + A^2 \ldots + A^a)(1 + B + \ldots + B^b)(1 + C + \ldots + C^c)\ldots.$$

Le nombre des diviseurs est égal au produit

$$(1 + a)(1 + b)(1 + c)\ldots.$$

La somme des diviseurs est égale au produit

$$\frac{A^{a+1} - 1}{A - 1} \cdot \frac{B^{b+1} - 1}{B - 1} \cdot \frac{C^{c+1} - 1}{C - 1} \cdots.$$

Remarque. — Le changement de A, B, C,... en $A^k, B^k, C^k, \ldots$, puis celui de $a, b, c, \ldots$ en $E\left(\frac{a}{k}\right), E\left(\frac{b}{k}\right), E\left(\frac{c}{k}\right), \ldots$ fait trouver les diviseurs qui sont des puissances d'exposant k, leur nombre et leur somme.

THÉORÈME. — *Le nombre des décompositions de* n *en deux facteurs conjugués d et $\frac{n}{d}$ est égal à la moitié de $(1 + a)(1 + b)(1 + c)\ldots$ si* n *n'est pas un carré, et à cette moitié $+\frac{1}{2}$ si* n *est un carré.*

THÉORÈME.—*Le nombre $n = A^a B^b C^c \ldots$ où les facteurs $A^a, B^b, C^c, \ldots$ sont au nombre de l, peut être décomposé en deux facteurs d, $\frac{n}{d}$ premiers entre eux, de 2^{l-1} manières.*

Dans ces deux théorèmes, $p \times q$ et $q \times p$ ne font qu'une même décomposition; pour effectuer ces décompositions, on prend pour premier facteur d un terme du produit

$$(a) \quad (1 + A + A^2 + \ldots + A^a)(1 + B + \ldots + B^b)(1 + C + \ldots + C^c)\ldots.$$

Dans le cas où les deux facteurs peuvent être quelconques, le deuxième facteur $\frac{n}{d}$ est aussi un terme du produit, différent du facteur d à moins que l'on n'ait $n = k^2$ et $d = k$; alors il faut ajouter $\frac{1}{2}$ à la moitié du produit $(1+a)(1+b)(1+c)\ldots$.

Dans le cas où les deux facteurs doivent être premiers entre eux, il faut prendre pour premier facteur d un terme du produit

$$(1+A^a)(1+B^b)(1+C^c)\ldots;$$

alors l'autre facteur $\frac{n}{d}$ est aussi un terme du même produit, et comme le nombre des termes est 2^l, le nombre demandé sera 2^{l-1}.

Théorème. — *Si les nombres $a, b, c,\ldots,$ sont décomposés en leurs facteurs de la forme A^α, B^β, $C^\gamma,\ldots$, 1° pour avoir le plus grand nombre qui divise chacun des nombres $a, b, c,\ldots,$ on prend le produit des nombres premiers $A, B, C,\ldots,$ qui entrent à la fois dans $a, b, c,\ldots,$ en leur donnant le moindre exposant qu'ils ont dans ces nombres; 2° pour avoir le moindre multiple des nombres $a, b, c,\ldots,$ on prend le produit de chacun des facteurs $A, B, C,\ldots$ qui entrent dans tous les nombres $a, b, c,\ldots,$ en donnant à chaque facteur premier le plus grand des exposants qu'il a dans ces nombres.*

Démonstration. — Pour le commun diviseur maximum, la règle donne un diviseur, et comme l'introduction d'un nouveau facteur premier, ou l'augmentation d'un exposant donnerait un nombre non diviseur commun, on a réellement le plus grand commun diviseur. Pour le moindre multiple commun, la règle donne effectivement un multiple, et comme la suppression d'un facteur ou la diminution d'un exposant donnerait un nombre qui ne serait pas multiple commun, on a réellement le moindre multiple commun.

23. Théorème. — *On a*

$$m(a,b) = \frac{ab}{D(a,b)},$$

$$m(a,b,c) = \frac{abc\,D(a,b,c)}{D(a,b)D(a,c)D(b,c)},$$

et généralement en représentant par P_1 le produit de n nombres $a, b, c,\ldots, l$, par P_2 le produit des $\frac{n(n-1)}{1.2}$ diviseurs $D(a,b)$ des n

nombres combinés 2 à 2; par P_3 *le produit des* $\frac{n(n-1)(n-2)}{1.2.3}$ *diviseurs* D (a, b, c) *des n nombres combinés* 3 *à* 3, *et ainsi de suite jusqu'à* P_n *qui ne contient que le terme* D $(a, b, c \ldots l)$,

$$m(a, b, c \ldots l) = \frac{P_1 P_3 \ldots P_n}{P_2 P_4 \ldots P_{n-1}} \quad \textit{pour n impair},$$

$$m(a, b, c \ldots l) = \frac{P_1 P_3 \ldots P_{n-1}}{P_2 P_4 \ldots P_n} \quad \textit{pour n pair}.$$

Démonstration. — Les nombres $a, b, c, \ldots, l$ étant rangés de manière qu'un certain facteur premier A y entre avec les exposants $\alpha, \beta, \gamma, \ldots, \lambda$, qui vont en décroissant, ou du moins non en augmentant, on verra tout de suite que l'exposant de A est égal

dans P_1 à... $e_1 = \alpha + \beta + \gamma + \delta + \ldots + \lambda$,

dans P_2 à... $e_2 = \beta + 2\gamma + 3\delta + \ldots + (n-1)\lambda$,

dans P_3 à... $e_3 = \gamma + 3\delta + \ldots + \frac{(n-1)(n-2)}{1.2}\lambda$,

dans P_4 à... $e_4 = \delta + \ldots + \frac{(n-1)(n-2)(n-3)}{1.2.3}\lambda$,

. . . .

Cela est évident pour le produit P_1. Pour les autres produits, les lettres étant rangées suivant l'ordre alphabétique, on voit que dans D (a, b) l'exposant de A est B comme dans b, que dans D (a, b, c) l'exposant de A est γ comme dans c, que dans D (a, b, c, d) l'exposant de A est δ comme dans d; ainsi dans le produit

$$P_2 = D(a, b) D(a, c) D(b, c) \ldots,$$

en cherchant combien il y a de nombres avant b, avant c, avant d, etc., on trouve que l'exposant de A est égal à

$$\beta + 2\gamma + 3\delta + \ldots + (n-1)\lambda.$$

Dans le produit

$$P_3 = D(a, b, c) D(a, b, d) D(b, c, d) \ldots,$$

en cherchant le nombre des combinaisons deux à deux des nombres

qui précèdent le dernier, on verra que l'exposant de A est

$$\gamma + 3\delta + \ldots + \frac{(n-1)(n-2)}{1.2}\lambda,$$

et ainsi de suite.

L'exposant de A dans $\frac{P_1P_3\ldots}{P_2P_4\ldots}$ sera donc

$$e = e_1 - e_2 + e_3 - e_4\ldots;$$

et dans cet exposant le multiplicateur de λ est égal à

$$1 - (n-1) + \frac{(n-1)(n-2)}{1.2} - \ldots.$$

Si l'on remplace $n-1$ par k, la somme algébrique

$$1 - k + \frac{k.(k-1)}{1.2} - \ldots = (1-1)^k = 0$$

représentera les coefficients de $\beta, \gamma, \delta, \ldots, \lambda$ dans e, selon qu'on aura

$$k = 1,\ 2,\ 3, \ldots, n-1.$$

L'exposant de A dans $\frac{P_1P_2\ldots}{P_2P_4\ldots}$ est donc α, exposant maximum de A.

On en peut dire autant de tout autre facteur premier, car l'ordre des nombres $a, b, c, \ldots$, peut être changé sans inconvénient.

26. Problème. — *Mettre les nombres a et b sous les formes*

$$a = a_1a_2, \quad b = b_1b_2,$$

a_1 *et* b_1 *n'ayant que des facteurs premiers diviseurs de a et b, et de plus* a_2 *étant premier à b et* b_2 *à a.*

Solution. — La décomposition en facteurs premiers donne immédiatement le résultat demandé, mais on peut le trouver par des recherches de plus grand commun diviseur, ainsi qu'il suit. On posera

$$a = a'\mathrm{D}(a, b), \quad b = b'\mathrm{D}(a, b),$$
$$a' = a''\mathrm{D}[a', \mathrm{D}(a, b)],$$
$$a'' = a'''\mathrm{D}\{a'', \mathrm{D}[a', \mathrm{D}(a, b)]\},$$

et ainsi de suite, et l'on aura

$$a = a' D(a, b),$$
$$a = a'' D[a', D(a, b)] . D(a, b),$$
$$a = a''' D\{a'', D[a', D(a, b)]\} . D[a', D(a, b)] . D(a, b),$$

et ainsi de suite. On a de même

$$b = b' D(a, b),$$
$$b = b'' D[b', D(a, b)] . D(a, b),$$
$$b = b''' D\{b'', D[b', D(a, b)]\} . D[b', D(a, b)] . D(a, b),$$

et ainsi de suite. L'opération se termine quand les diviseurs communs sont égaux à l'unité.

Remarque. — La recherche du moindre multiple s'étend très-facilement aux polynômes algébriques

$$f(x) = x^m + ax^{m-1} + \ldots + fx + g = (x - r_1)(x - r_2)\ldots(x - r_m),$$

décomposés en facteurs du premier degré réels ou imaginaires, car les facteurs $x - r_1$, $x - r_2, \ldots$, peuvent être considérés comme premiers.

27. Théorème. — *En désignant par $\varphi(m)$ le nombre des entiers non supérieurs et premiers à $m = A^a B^b C^c \ldots$, on a $\varphi(1) = 1$ et*

$$\varphi(m) = A^{a-1}(A - 1) B^{b-1}(B - 1) C^{c-1}(C - 1)\ldots$$
$$= m\left(\frac{A-1}{A}\right)\left(\frac{B-1}{B}\right)\left(\frac{C-1}{C}\right)\ldots$$
$$= m\left(1 - \frac{1}{A}\right)\left(1 - \frac{1}{B}\right)\left(1 - \frac{1}{C}\right)\ldots.$$

Démonstration. — Pour trouver les entiers inférieurs et premiers à m, il suffit de supprimer dans la suite $1, 2, 3, \ldots, m$ les multiples de A, puis ceux de B qui ne le sont pas de A, puis ceux de C qui ne le sont ni de A, ni de B, et ainsi de suite.

Or les multiples de A sont

$$A, 2A, 3A, 4A, \ldots, \frac{m}{A} A$$

au nombre de $\frac{m}{A}$: il reste donc

$$m - \frac{m}{A} = m\left(1 - \frac{1}{A}\right)$$

nombres non multiples de A.

Les multiples de B sont

$$B, 2B, 3B, \ldots, \frac{m}{B}B,$$

au nombre de $\frac{m}{B}$; mais parmi eux il y a des multiples de A au nombre de $\frac{m}{AB}$, il reste donc $\frac{m}{B}\left(1-\frac{1}{A}\right)$ multiples de B à supprimer; par conséquent

$$m\left(1-\frac{1}{A}\right)-\frac{m}{B}\left(1-\frac{1}{A}\right)=m\left(1-\frac{1}{A}\right)\left(1-\frac{1}{B}\right)$$

indique combien au-dessous de m il y a de nombres premiers à A et à B.

De même, comme parmi les nombres

$$C, 2C, 3C, \ldots, \frac{m}{C}C,$$

il y en a

$$\frac{m}{C}\left(1-\frac{1}{A}\right)\left(1-\frac{1}{B}\right)$$

premiers avec A et B, suppression faite, il restera

$$m\left(1-\frac{1}{A}\right)\left(1-\frac{1}{B}\right)-\frac{m}{C}\left(1-\frac{1}{A}\right)\left(1-\frac{1}{B}\right)$$
$$=m\left(1-\frac{1}{A}\right)\left(1-\frac{1}{B}\right)\left(1-\frac{1}{C}\right)$$

nombres premiers à A, B, C, et ainsi de suite.

Remarque. — Pour $m=A^a$ on a

$$\varphi(A^a)=A^{a-1}(A-1),$$

et par suite

$$\varphi(A^a.B^b.C^c\ldots)=\varphi(A^a).\varphi(B^b).\varphi(C^c)\ldots.$$

En général, si $l, m, n, \ldots$ sont premiers entre eux deux à deux, on aura

$$\varphi(l.m.n\ldots)=\varphi(l).\varphi(m).\varphi(n)\ldots.$$

28. Théorème. — *On a, pour toute valeur de m, $\Sigma\varphi(d)=m$, la somme s'étendant à tous les nombres d diviseurs de m.*

Démonstration. — Soit $m=A^aB^bC^c\ldots$; les nombres d diviseurs de m sont les termes du produit

$$(1+A+A^2+\ldots+A^a)(1+B+B^2\ldots+B^b)(1+C+C^2+\ldots+C^c)\ldots.$$

Tout nombre $\varphi(d)$ est un terme du produit

$$[1+\varphi(A)+\varphi(A^2)+\ldots+\varphi(A^a)][1+\varphi(B)+\ldots+\varphi(B^b)]$$
$$[1+\varphi(C)+\ldots+\varphi(C^c)]\ldots,$$

et, comme on a

$$1+\varphi(A)+\varphi(A^2)+\ldots+\varphi(A^a)=1+(A-1)(A^{a-1}+\ldots+A+1)=A^a,$$
$$1+\varphi(B)+\ldots+\varphi(B^b)=B^b,$$

et ainsi des autres, il en résulte que

$$\Sigma\varphi(d)=m.$$

29. Théorème. — *Le produit* Πn *contient le facteur premier* P *avec l'exposant*

$$e=E\left(\frac{n}{P}\right)+E\left(\frac{n}{P^2}\right)+E\left(\frac{n}{P^3}\right)+\ldots+E\left(\frac{n}{P^i}\right),$$

en supposant

$$P^{i+1}>n\geqq P^i,$$

Démonstration. — Pour avoir l'exposant de P dans Πn, il suffit de considérer le produit

$$P.2P.3P\ldots E\left(\frac{n}{P}\right).P=1.2.3\ldots E\left(\frac{n}{P}\right).P^{E\left(\frac{n}{P}\right)},$$

des facteurs multiples de P. De même au lieu de $1.2.3\ldots E\left(\frac{n}{P}\right)$, on prendra le produit

$$P.2P.3P\ldots E\left(\frac{n}{P^2}\right).P=1.2.3\ldots E\left(\frac{n}{P^2}\right).P^{E\left(\frac{n}{P^2}\right)},$$

et ainsi de suite, de sorte qu'on aura

$$P^{E\left(\frac{n}{P}\right)+E\left(\frac{n}{P^2}\right)+\ldots+E\left(\frac{n}{P^i}\right)}$$

pour la plus haute puissance de P qui divise Πn.

Remarque. — Si l'on fait

$$n=a+bP+cP^2+dP^3\ldots,$$

$a, b, c,\ldots,$ étant positifs ou nuls, mais inférieurs à P, en calculant

les nombres $E\left(\frac{n}{P}\right)$, $E\left(\frac{n}{P^2}\right)$, etc., on trouvera

$$e = \frac{n-(a+b+c\ldots)}{P-1}.$$

L'expression $\frac{n}{P-1}$ est une limite supérieure, quelquefois utile.

Théorème. — *Si l'on pose*

$$n = a+b+c+\ldots,$$

il en résultera

$$\frac{n}{P^i} = \frac{a}{P^i} + \frac{b}{P^i} + \frac{c}{P^i} + \cdots;$$

et par suite

$$E\left(\frac{n}{P^i}\right) = \text{ou} > E\left(\frac{a}{P^i}\right) + E\left(\frac{b}{P^i}\right) + E\left(\frac{c}{P^i}\right)\cdots.$$

Théorème. — *L'expression*

$$\frac{\Pi(a+b+c\ldots)}{\Pi a.\Pi b.\Pi c\ldots}$$

est un nombre entier.

Car les deux théorèmes précédents montrent que l'exposant de P au numérateur est au moins égal à celui de P au dénominateur.

30. Théorème. — *Si l'on représente par* $P(x)$ *le produit* 2.3.5.7... *des nombres premiers non supérieurs à* x, *et par* P_k *le produit*

$$P(\sqrt[k]{n}).P\left(\sqrt[k]{\frac{n}{2}}\right).P\left(\sqrt[k]{\frac{n}{3}}\right).P\left(\sqrt[k]{\frac{n}{4}}\right)\cdots$$

où $\left(\sqrt[k]{\frac{n}{h}}\right)$ *est mis pour* $E\left(\sqrt[k]{\frac{n}{h}}\right)$, *l'exposant du nombre premier* N *dans* P_k *est l'entier* $E\left(\frac{n}{N^k}\right)$.

Démonstration. — Chaque produit $P\left(\sqrt[k]{\frac{n}{h}}\right)$ ne renferme un nombre premier qu'une fois. Si N entre dans le produit $P\left(\sqrt[k]{\frac{n}{h}}\right)$, il entrera à plus forte raison dans les précédents. Il faut donc exprimer

que l'on a

$$\sqrt[k]{\frac{n}{h+1}} < N \leqq \sqrt[k]{\frac{n}{h}},$$

d'où l'on tire

$$n < (h+1)N^k, \quad n \geqq hN^k,$$

ce qui revient à

$$h = E\left(\frac{n}{N^k}\right).$$

Ce nombre h est évidemment l'exposant de N dans P_k.

Théorème. — *On a*

$$(a)\quad \left\{\begin{array}{l} \Pi n = P(n).P\left(\frac{n}{2}\right).P\left(\frac{n}{3}\right)\cdots\cdot \\ \quad \times P(\sqrt{n}).P\left(\sqrt{\frac{n}{2}}\right).P\left(\sqrt{\frac{n}{3}}\right)\cdots \\ \quad \times P\sqrt[3]{(n)}.P\left(\sqrt[3]{\frac{n}{2}}\right).P\left(\sqrt[3]{\frac{n}{3}}\right)\cdots \\ \quad \cdots\cdots\cdots\cdots\cdots\cdots \\ \quad \times P(\sqrt[p]{n}).P\left(\sqrt[p]{\frac{n}{2}}\right).P\left(\sqrt[p]{\frac{n}{3}}\right)\cdots\cdot \end{array}\right.$$

On s'arrête quand on a $\sqrt[p]{n} < 2$, c'est-à-dire $n < 2^p$.

Démonstration. — L'exposant du nombre premier N est, d'après le théorème précédent, $E\left(\frac{n}{N}\right)$ dans la première ligne, $E\left(\frac{n}{N^2}\right)$ dans la seconde, $E\left(\frac{n}{N^3}\right)$ dans la troisième, etc.

On a donc pour exposant de N dans le second membre de l'équation (a)

$$e = E\left(\frac{n}{N}\right) + E\left(\frac{n}{N^2}\right) + E\left(\frac{n}{N^3}\right) + \ldots,$$

précisément comme dans le produit Πn.

Ce dernier théorème a été trouvé par MM. Tchebichew et A. de Polignac, qui en ont fait usage dans leurs recherches sur les nombres premiers.

La formule de M. Tchebichew s'obtient en prenant les logarithmes des deux membres de l'équation (a).

Remarque. — Si l'on pose

$$P(n).P(\sqrt{n}).P(\sqrt[3]{n})\ldots = P_1(n),$$

on obtiendra

$$\Pi n = P_1(n).P_1\left(\frac{n}{2}\right).P_1\left(\frac{n}{3}\right)\cdots$$

Au moyen de cette formule et en partant de deux limites du produit Πn, ou de son logarithme, M. Tchebichew a trouvé deux limites de $P(n)$. *Voyez* son Mémoire sur les nombres premiers (*Journal de Mathématiques,* tome XVII). La considération des deux limites de $P(n)$ conduit à divers théorèmes, et entre autres à celui-ci : *Au delà de* $a = 3$ *il y a au moins un nombre premier entre* a *et* $2a - 2$. Dans son Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme (*Journal de l'École Polytechnique,* 30[e] cahier), M. J. Bertrand avait admis cette proposition comme *Postulatum.*

On tire de là différentes conséquences. Ainsi comme l'a montré M. Liouville, le produit

$$\Pi n = 1.2.3\ldots n$$

ne saurait être une puissance (carré, cube, etc.), ni un produit de puissances, puisqu'il y a au moins un nombre premier qui n'y entre qu'une fois comme facteur (*Journal de Mathématiques,* t. II, 2[e] série).

La démonstration de M. Tchebichew est probablement susceptible de simplification et de généralisation. On peut voir à ce sujet divers articles du prince A. de Polignac, insérés dans les *Comptes rendus des séances de l'Académie des Sciences.*

Les propriétés des nombres composés se déduisant de celles des nombres premiers, il est fort important de perfectionner et de simplifier la théorie des nombres premiers; ce sujet, qui présente de grandes difficultés, sera repris dans un des Mémoires qui suivront cette Introduction.

CHAPITRE V.

DES FONCTIONS ENTIÈRES. — DES FONCTIONS HOMOGÈNES. — PROPOSITIONS ÉLÉMENTAIRES.

31. Les recherches sur les nombres concernent surtout ceux qui résultent des fonctions entières à une ou plusieurs variables, quand on donne aux variables des valeurs entières. Ainsi $a, b, c, \ldots$ étant des nombres entiers positifs ou négatifs, on considère les fonctions suivantes :

La fonction du premier degré $ax+b$, ou la forme linéaire des nombres. Quand on y fait

$$x = \ldots -3, \quad -2, \quad -1, \quad 0, \quad 1, \quad 2, \quad 3, \ldots,$$

on a des nombres en progression arithmétique. La formule $3x+2$ donne par ces substitutions

$$\ldots -7, \quad -4, \quad -1, \quad 2, \quad 5, \quad 8, \quad 11, \ldots$$

La différence entre deux termes consécutifs est constante. Pour $ax+b$ on a

$$a(x+1)+b-(ax+b) = a.$$

La fonction entière du second degré ax^2+bx+c. Si l'on donne à x les valeurs consécutives $\ldots -2, -1, 0, 1, 2, 3, \ldots$, on obtiendra des nombres en progression arithmétique du second ordre, les différences des termes consécutifs formeront une progression arithmétique ordinaire. Voici l'exemple le plus simple, celui de la fonction x^2 :

x.......	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,
x^2......	0,	1,	4,	9,	16,	25,	36,	49,	64,	81,	100,
Diff. 1re..		1,	3,	5,	7,	9,	11,	13,	15,	17,	19,
Diff. 2e..			2,	2,	2,	2,	2,	2,	2,	2,	2.

Les différences secondes sont constantes. La fonction étant ax^2, la différence est $2a$.

Généralement, pour $ax^2 + bx + c$, la différence est

$$a(x+1)^2 + b(x+1) + c - (ax^2 + bx + c) = a(2x+1) + b = 2ax + a + b.$$

Les différences premières sont en progression arithmétique dont la raison est $2a$ et les différences secondes sont constantes et égales à $1.2a$.

La fonction du troisième degré $ax^3 + bx^2 + cx + d$ donne des nombres en progression arithmétique du troisième ordre, dont les différences troisièmes sont constantes, car les différences premières étant

$$a[(x+1)^3 - x^3] + b[(x+1)^2 - x^2) + c(x + 1 - x),$$

ou

$$a(3x^2 + 3x + 1) + b(2x + 1) + c = 3ax^2 + (3a + 2b)x + a + b + c,$$

on voit que les différences troisièmes sont constantes et égales à $1.2.3a$.

En général, pour la fonction entière de degré m, on a des nombres en progression arithmétique du $m^{ième}$ ordre dont les $m^{ièmes}$ différences sont constantes. Pour la fonction $ax^m + bx^{m-1} + \ldots + fx + g$, cette différence est $1.2.3\ldots ma$.

N. B. Si au lieu de substituer pour x la suite des nombres naturels 1, 2, 3, etc., on mettait des nombres en progression arithmétique de raison h, la différence $m^{ième}$, pour la fonction du $m^{ième}$ degré $ax^m + bx^{m-1} \ldots + fx + g$, serait $1.2.3\ldots mah^m$.

Si l'on représente par

$$u_0, \quad u_1, \quad u_2, \quad u_3, \ldots, u_n$$

une suite de nombres et que leurs différences

$$u_1 - u_0, \quad u_2 - u_1, \ldots, \quad u_n - u_{n-1}$$

soient désignées par

$$\Delta u_0, \quad \Delta u_1, \ldots, \quad \Delta u_{n-1},$$

puis leurs différences secondes

$$\Delta u_1 - \Delta u_0, \quad \Delta u_2 - \Delta u_1, \ldots, \quad \Delta u_{n-1} - \Delta u_{n-2}$$

par

$$\Delta^2 u_0, \qquad \Delta^2 u_1, \ldots, \qquad \Delta^2 u_{n-2},$$

et ainsi de suite, on déduira facilement de ces notations

$$u_1 = u_0 + \Delta u_0,$$
$$u_2 = u_0 + 2\Delta u_0 + \Delta^2 u_0,$$
$$u_3 = u_0 + 3\Delta u_0 + 3\Delta^2 u_0 + \Delta^3 u_0,$$

et généralement

$$u_k = u_0 + k\Delta u_0 + \frac{k(k-1)}{1.2}\Delta^2 u_0 + \ldots + k\Delta^{k-1} u_0 + \Delta^k u_0,$$

On trouvera semblablement

$$\Delta u_0 = u_1 - u_0,$$
$$\Delta^2 u_0 = u_2 - 2u_1 + u_0,$$
$$\Delta^3 u_0 = u_3 - 3u_2 + 3u_1 - u_0,$$

et généralement

$$\Delta^k u_0 = u_k - k u_{k-1} + \frac{k(k-1)}{1.2} u_{k-2} - \ldots \pm k u_1 \mp u_0.$$

Ces formules, utiles dans plusieurs questions, sont exposées avec tous les développements nécessaires dans les Traités d'algèbre.

32. On peut se proposer, relativement à la fonction entière

$$f(x) = ax^n + bx^{n-1} + \ldots + fx + g,$$

diverses questions, notamment celles-ci : Quels sont les nombres qui mis pour x rendent $f(x)$ divisible par un nombre donné m; autrement, résoudre en nombres entiers l'équation indéterminée

$$f(x) = my.$$

Toute une partie de la théorie des nombres ou plutôt de l'analyse indéterminée traite de cette équation qu'on nomme *congruence*.

Une autre question qui se rattache à la précédente est de trouver la forme des nombres m qui divisent une fonction entière $f(x)$. Ces questions sont loin d'être résolues complétement et d'une manière réellement pratique.

Voici une transformation de $f(x)$ souvent utile.

THÉORÈME. — *Si l'on a*

$$f(x) = ax^n + bx^{n-1} + \ldots + fx + g,$$

il en résultera

$$f(x)-f(\alpha)=(x-\alpha)\,[ax^{n-1}+(a\alpha+b)\,x^{n-2}$$
$$+(a\alpha^2+b\alpha+c)x^{n-3}+\ldots+a\,\alpha^{n-1}+b\,\alpha^{n-2}+c\alpha^{n-3}+\ldots$$
$$+f\alpha+g].$$

Démonstration. — Cela résulte de la formule

$$x^n-\alpha^n=(x-\alpha)\,[x^{n-1}+\alpha x^{n-2}+\alpha^2x^{n-3}+\ldots+\alpha^{n-2}x+\alpha^{n-1}].$$

Cette transformation peut encore être présentée autrement. Si l'on nomme fonction dérivée de $f(x)$ et qu'on représente par $f'(x)$ une fonction tirée de la fonction entière $ax^n+bx^{n-1}+\ldots+fx+g$, en multipliant chaque terme par l'exposant de x, puis diminuant cet exposant de l'unité, on aura

$$f'(x)=nax^{n-1}+(n-1)\,bx^{n-2}+\ \ldots+f.$$

Si $f''(x)$ représente semblablement la dérivée de $f'(x)$, de sorte qu'on ait

$$f''(x)=n(n-1)\,ax^{n-2}+(n-1)(n-2)\,bx^{n-3}+\ldots,$$

et ainsi de suite; si l'on remplace x par $\alpha+(x-\alpha)$ et qu'on développe les puissances

$$[\alpha+(x-\alpha)]^k$$

par la formule du binôme, on aura la proposition suivante :

THÉORÈME. — *La fonction entière $f(x)$ se développe ainsi :*

$$f(x)=f(\alpha)+f'(\alpha)\,(x-\alpha)+\frac{f''(\alpha)}{1.\,2}(x-\alpha)^2+\frac{f'''(\alpha)}{1.2.3}(x-\alpha)^3+\ldots$$
$$+\frac{f^{n-1}(\alpha)}{1.2\ldots n-1}(x-\alpha)^n+\frac{f^{(n)}(\alpha)}{1.2.3\ldots n}(x-\alpha)^n,$$

ce qui revient à

$$f(x)-f(\alpha)=(x-\alpha)\left[f'(\alpha)+\frac{f''(\alpha)}{1.2}(x-\alpha)+\ldots+\frac{f^n(\alpha)}{1.2\ldots n}(x-\alpha)^{n-1}\right].$$

33. Après les fonctions entières d'une seule variable viennent les fonctions entières de plusieurs et principalement les fonctions algébriques. Il faut distinguer surtout les fonctions homogènes. Les fonctions

$$ax+by,\quad ax+by+cz,\quad ax+by+cz+du,\ \text{etc.},$$

sont des fonctions homogènes du premier degré.

Après les fonctions homogènes du premier degré viennent celles du second, à deux ou plusieurs variables,

$$ax^2 + bxy + cy^2,$$
$$ax^2 + by^2 + cz^2 + dyz + ezx + fxy,$$

et ainsi de suite.

Ces fonctions homogènes du second degré sont dites *quadratiques, et binaires, ternaires, quaternaires, etc.*, selon le nombre des variables.

Comme les fonctions entières non homogènes se partagent en fonctions homogènes de divers degrés, on voit que leurs proprietés doivent dériver de celles des fonctions homogènes.

34. En multipliant une fonction homogène de degré m par une fonction homogène de degré n on trouve une fonction homogène de degré $m+n$.

Voici des exemples qui serviront plus loin :

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= a^2c^2+b^2c^2+a^2d^2+b^2d^2\\ &= (a^2c^2+b^2d^2)+(b^2c^2+a^2d^2)\\ &= (ac\pm bd)^2+(bc\mp ad)^2.\end{aligned}$$

Cette transformation s'obtient par l'addition de la quantité nulle

$$2\,ac.\,bc - 2\,bc.ad,$$

ou par la soustraction de la même quantité.

On voit donc qu'une somme de deux carrés, multipliée par une somme de deux carrés, donne de deux manières une autre somme de deux carrés. Mais il peut y avoir d'autres décompositions en deux carrés; ce qui précède n'est qu'une simple vérification. Cette formule a été donnée par Léonard de Pise dans son livre des carrés retrouvé par les soins du prince Boncompagni.

Euler a donné la formule

$$\begin{aligned}(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = {} & (aA+bB+cC+dD)^2,\\ & +(aB-bA+cD-dC)^2,\\ & +(aC-bD-cA+dB)^2,\\ & +(aD+bC-cB-dA)^2,\end{aligned}$$

qui montre qu'une somme de quatre carrés, multipliée par une somme de quatre carrés, donne une somme de quatre carrés. Comme il est permis de changer le signe d'un ou de plusieurs des nombres

a, b, c, d; A, B, C, D, ce qui ne change pas le premier membre, on a diverses décompositions.

La formule suivante, qui est de Lagrange, renferme celle d'Euler :

$$\begin{aligned}(p^2 - Bq^2 - Cr^2 + BCs^2)(p'^2 - Bq'^2 - Cr'^2 + BCs'^2) \\ = (pp' + Bqq' \pm C rr' \pm BCss')^2 \\ - B(pq' + p'q \pm Crs' \pm Cr's)^2 \\ - C(pr' - Bqs' \pm rp' \mp Bsq')^2 \\ + BC(qr' - ps' \pm p's \mp rq')^2.\end{aligned}$$

En faisant $B = C = -1$, on retrouve la formule d'Euler, à la notation près.

Il existe des formules analogues pour des degrés supérieurs.

M. Brioschi a donné une formule pour le cas du produit de huit carrés par huit carrés, probablement la suivante avec quelques changements de signe :

$$\begin{aligned}(a^2+b^2+c^2+d^2+e^2+f^2+g^2+h^2)(a'^2+b'^2+c'^2+d'^2+e'^2+f'^2+g'^2+h'^2) \\ = (aa' + bb' + cc' + dd' + ee' + ff' + gg' + hh')^2 \\ + (ab' - ba' - cd' + dc' - ef' + fe' - gh' + hg')^2 \\ + (ac' + bd' - ca' - db' + eg' - fh' - ge' + hf')^2 \\ + (ad' - bc' + cb' - da' - eh' - fg' + gf' + he')^2 \\ + (ae' + bf' - cg' + dh' - ea' - fb' + gc' - hd')^2 \\ + (af' - be' + ch' + dg' + eb' - fa' - gd' - hc')^2 \\ + (ag' + bh' + ce' - df' - ec' + fd' - ga' - hb')^2 \\ + (ah' - bg' - cf' - de' + ed' + fc' + gb' - ha')^2.\end{aligned}$$

Cette formule m'a été communiquée par M. Prouhet.

La proposition s'étend au produit de la somme de 2^m carrés par celle de 2^m carrés, qui est aussi formé de 2^m carrés, comme l'a montré M. Angelo Genocchi (*Annali di Matematica pura ed applicata*, t. III, n° 4.)

38. Les démonstrations précédentes sont purement arithmétiques; on pourrait aussi employer la considération des imaginaires; ainsi

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) = (a + b\sqrt{-1})(a - b\sqrt{-1})(c + d\sqrt{-1})(c - d\sqrt{-1}) \\ = (a + b\sqrt{-1})(c + d\sqrt{-1}) \times (a - b\sqrt{-1})(c - d\sqrt{-1}) \\ = [(ac - bd) + (ad + bc)\sqrt{-1}][ac - bd - (ad + bc)\sqrt{-1}] \\ = (ac - bd)^2 + (ad + bc)^2.\end{aligned}$$

C'est là une démonstration analytique.

Voici une autre démonstration de même genre.

Si l'on pose

$$a^2+b^2=(a+b\sqrt{-1})(a-b\sqrt{-1}),$$

il en résultera

$$\begin{aligned}(a^2+b^2)^m &= (a+b\sqrt{-1})^m(a-b\sqrt{-1})^m\\ &= (A+B\sqrt{-1})(A-B\sqrt{-1})\\ &= A^2+B^2,\end{aligned}$$

en posant, d'après la formule du binôme,

$$A=a^m-\frac{m(m-1)}{1.2}a^{m-2}b^2+\ldots,$$

$$B=ma^{m-1}b-\frac{m(m-1)(m-2)}{1.2.3}a^{m-3}b^3+\ldots.$$

On voit par cet exemple comment l'emploi des imaginaires abrége certains calculs.

Il serait facile d'obtenir d'autres résultats par la multiplication, mais on n'en verrait pas immédiatement l'usage; il suffira d'en citer quelques-uns d'un emploi fréquent :

$$(a-b)(a^{m-1}+a^{m-2}b+a^{m-3}b^2+\ldots+ab^{m-2}+b^{m-1})=a^m-b^m.$$

Le changement de b en $-b$ donne, pour m pair,

$$(a+b)(a^{m-1}-a^{m-2}b+a^{m-3}b^2-\ldots+ab^{m-2}-b^{m-1})=a^m-b^m,$$

et, pour m impair,

$$(a+b)(a^{m-1}-a^{m-2}b+a^{m-3}b^2-\ldots-ab^{m-2}+b^{m-1})=a^m+b^m.$$

Si l'on fait $b=1$, la formule

$$(a-1)(a^{m-1}+a^{m-2}+\ldots+a+1)=a^m-1$$

donne la somme des nombres

$$1,\quad a,\quad a^2,\ldots,\quad a^{m-1},$$

qui forment une progression géométrique.

36. Parmi les fonctions transcendantes, la théorie des nombres considère surtout la fonction a^x; en y faisant $x=0, 1, 2, 3, 4$, etc.,

on a une suite de nombres en progression géométrique

$$1, \quad a, \quad a^2, \quad a^3, \ldots, \quad a^x,$$

dont la somme des termes est $\frac{a^{x+1}-1}{a-1}$.

Les différences successives de ces nombres sont aussi des progressions géométriques, comme on le voit ci-dessous :

$$\begin{array}{lllll}
1, & a, & a^2, & a^3, & a^4, \ldots, \\
 & (a-1), & a(a-1), & a^2(a-1), & a^3(a-1), \ldots, \\
 & & (a-1)^2, & a(a-1)^2, & a^2(a-1)^2, \ldots, \\
 & & & (a-1)^3, & a(a-1)^3, \ldots, \\
 & & & & (a-1)^4, \ldots, \\
\ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

Leurs premiers termes forment encore une progression géométrique

$$(a-1), \quad (a-1)^2, \quad (a-1)^3, \quad (a-1)^4, \ldots.$$

Quand on considère les restes des nombres

$$1, \quad a, \quad a^2, \quad a^3, \ldots,$$

divisés par un même nombre, on est conduit à certaines propositions d'où résulte une sorte de logarithmes aussi utiles en pratique qu'en théorie.

CHAPITRE VI.

DE LA CONGRUENCE DES NOMBRES. — THÉORÈMES ÉLÉMENTAIRES.

37. Le nombre *positif* m étant pris pour *module* ou pour terme de comparaison, si pour un nombre quelconque n on pose

$$n = mq + r,$$

le nombre r, quels que soient son signe et sa grandeur, est dit *résidu* de n pour le *module* m. Si le nombre q est déterminé de manière que r soit en valeur absolue inférieur à m, ce qui arrive quand mq est l'un des deux multiples consécutifs de m, entre lesquels tombe n, on dit que r est un *résidu minimum*.

Le résidu minimum positif étant r, le nombre $r - m = -(m - r)$ est le résidu minimum négatif. La somme des valeurs absolues de ces deux résidus r et $m - r$ est donc m. Quand n est multiple de m, il n'y a qu'un résidu minimum égal à zéro.

On dit que deux nombres sont congrus pour le module m, quand ils sont réductibles à une même forme $mx + r$, r étant un résidu qu'on prendra généralement minimum.

Les nombres $n = m\alpha + r$, $n' = m\beta + r$ sont donc congrus; cette congruence s'exprime ainsi

$$n \equiv n' \text{ mod. } m,$$

ce qui revient à l'équation

$$n - n' = m(\alpha - \beta),$$

qu'on peut mettre sous ces deux formes

$$n = m(\alpha - \beta) + n' \quad \text{ou} \quad n' = m(\beta - \alpha) + n.$$

On peut donc dire indifféremment que n est résidu de n', ou n' de n, pour le module m.

Tous les nombres sont compris dans les formules

$$mx,\quad mx+1,\quad mx+2,\ldots,\quad mx+m-1.$$

Les nombres

$$0,\quad 1,\quad 2,\quad 3,\ldots,\quad m-1$$

forment un système de restes.

Comme les formules

$$mx+m-1,\quad mx+m-2,\quad mx+m-3\ldots$$

reviennent à

$$m(x+1)-1,\quad m(x+1)-2,\quad m(x+1)-3,\ldots,$$

on peut dire que, pour avoir tous les nombres possibles, il suffit de considérer m formules consécutives parmi les suivantes :

$$\ldots mx-2,\quad mx-1,\quad mx,\quad mx+1,\quad mx+2\ldots,$$

et, si l'on prend m nombres consécutifs parmi les suivants

$$\ldots -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3\ldots,$$

on aura encore un système de résidus.

38. Au moyen de ces remarques on reconnaîtra tout de suite la vérité des propositions suivantes :

Théorèmes. — *Les nombres congrus à un même nombre sont congrus entre eux. Les nombres congrus suivant le module* n *le sont aussi suivant les diviseurs de* m. *Les nombres congrus suivant les modules* $m, m', m'',\ldots,$ *premiers entre eux deux à deux, le sont suivant le produit* $m\,m'\,m''\ldots.$

Si l'on a

$$ka \equiv kb \text{ mod.} m \quad \text{ou} \quad k(a-b) \equiv 0 \text{ mod.} m,$$

et que k *soit premier à* m, *on aura*

$$a \equiv b \text{ mod.} m,$$

car $a-b$ est divisible par m.

Théorème. — *Si l'on a*

$$a \equiv \alpha,\quad b \equiv \beta,\quad c \equiv \gamma,\ldots \text{ mod.} m,$$

on aura aussi pour le module m

$$a \pm b \equiv \alpha \pm \beta,\quad a+b+c \equiv \alpha+\beta+\gamma,\quad a^k \equiv \alpha^k,\quad abc\ldots \equiv \alpha\beta\gamma\ldots$$

Généralement, si

$$F(x),\quad F(x,y),\quad F(x,y,z),\ldots$$

sont des fonctions entières à coefficients entiers, on aura

$$F(a) \equiv F(\alpha),\quad F(a,b) \equiv F(\alpha,\beta),\quad F(a,b,c) \equiv F(\alpha,\beta,\gamma)\ldots \bmod. m.$$

Démonstration. — On le voit immédiatement en remplaçant

$$a \equiv \alpha,\quad b \equiv \beta,\quad c \equiv \gamma,\quad \bmod. m$$

par

$$a = \alpha + mg,\quad b = \beta + mg',\quad c = \gamma + mg''.$$

Théorème. — *Si dans* $F(x)$ *on met pour* x *la suite des nombres entiers et qu'on prenne les résidus minima, ils se reproduiront périodiquement : ce seront les restes de*

$$F(0),\quad F(1),\quad F(2)\ldots F(m-1),$$

le module étant m.

Corollaire. — Si le reste r ne se présente pas, la congruence $F(x) \equiv r$ est impossible.

59. Gauss se proposait de développer ce caractère d'impossibilité dans la huitième section de ses *Recherches arithmétiques.* On peut présumer qu'il voulait aussi parler de l'impossibilité des équations indéterminées à plusieurs inconnues.

Quand $F(x, y, z\ldots) = 0$ pour des valeurs entières $x = a$, $y = b$, $z = c\ldots$, à plus forte raison la congruence

$$F(x, y, z\ldots) \equiv 0,$$

a lieu pour un module quelconque. Donc si, pour un module convenablement choisi, la congruence est impossible, on en devra conclure l'impossibilité de l'équation $F(x,y,z\ldots) = 0$.

Pour le cas de $F(x)$, Gauss prend l'exemple

$$F(x) = x^3 - 8x + 6;$$

alors, pour le module 5, on a

$$F(0) \equiv 1,\quad F(1) \equiv 4,\quad F(2) \equiv 3,\quad F(3) \equiv 4,\quad F(4) \equiv 3;$$

on aurait pu prendre

$$F(-2),\quad F(-1),\quad F(0),\quad F(1),\quad F(2)\quad \text{ou}\quad 4,\quad 3,\quad 1,\quad 4,\quad 3.$$

Comme les restes o et 2 ne se présentent pas, on voit qu'on ne saurait résoudre en nombres entiers les congruences

$$x^3 - 8x + 6 \equiv 0, \quad x^3 - 8x + 6 \equiv 2 \text{ mod. } 5,$$

et par suite les équations

$$x^3 - 8x + 6 = 0, \quad x^3 - 8x + 4 = 0.$$

Voici d'autres exemples d'impossibilité, souvent employés :

Les congruences

$$x^2 \equiv 2,\ 3,\ 4,\ 5,\ 6,\ 7, \text{ mod. } 8 \text{ sont impossibles;}$$

autrement, *un carré ne saurait avoir les formes*

$$8k + 2, \quad 8k + 3, \quad 8k + 5, \quad 8k + 6, \quad 8k + 7.$$

De même les congruences

$$x^2 \equiv 2,\ 3,\ 5,\ 6,\ 7,\ 8,\ 10,\ 11, \text{ mod. } 12$$

sont impossibles; autrement, *il n'y a pas de carré des formes*

$$12k + 2,\ 3,\ 5,\ 6,\ 7,\ 8,\ 10,\ 11,$$

et ainsi de suite pour tous les modules.

Théorème. — *L'équation $x^4 + y^4 = z^2$ est impossible en nombres entiers quand l'inconnue paire n'est pas divisible par* 4.

Démonstration. — Il suffit de montrer qu'elle est impossible pour certains modules, c'est ce qui se fait comme il suit :

1° On peut supposer que x et y n'ont aucun facteur commun, car s'il existait, on le ferait disparaître par la division. Par suite, x et z, y et z n'en auront pas non plus.

2° Les nombres x, y, z ne sont pas tous impairs, car si cela était, un membre serait pair et l'autre impair; il n'y aurait pas congruence pour le module 2.

3° Un seul des nombres x, y, z peut être pair et ce n'est pas z, car il n'y aurait pas, pour z pair, congruence pour le module 4, le premier membre ayant la forme $4k + 2$, et le second la forme $4k$.

4° Soit x pair; il y aura impossibilité pour x double d'un impair p. Dans ce cas, $x = 2p$ donne

$$16p^4 = z^2 - y^4 = (z - y^2)(z + y^2);$$

comme les facteurs $z - y^2$, $z + y^2$ ont pour somme $2z$, et pour dif-

férence $2y^2$, leur plus grand commun diviseur est 2; on devra donc poser

$$z \pm y^2 = 2r^4, \quad z \mp y^2 = 8s^4, \quad p = rs, \quad D(r,s) = 1,$$

et de là, par soustraction,

$$\pm y^2 = r^4 - 4s^4.$$

Il faudra prendre le signe supérieur pour que les deux membres soient de la même forme $4k+1$; on a donc

$$4s^4 = r^4 - y^2;$$

équation impossible, le premier membre ayant la forme $8k+4$ et le second la forme $8f$.

THÉORÈME. — *L'équation*

$$(2^a x)^4 + y^4 = z^2,$$

x étant impair, se ramène à l'équation

$$(2^{a-1} x_1)^4 + y_1^4 = z_1^2,$$

de sorte qu'en définitive on retombe sur le cas précédent, et l'impossibilité est généralement démontrée.

Démonstration. — Soit

$$x = pq; \quad 2^{4a} p^4 q^4 = (z \pm y^2)(z \mp y^2).$$

De là

$$2p^4 = z \pm y^2, \quad 2^{4a-1} q^4 = z \mp y^2; \quad \text{d'où} \quad p^4 - 2^{4a-2} q^4 = \pm y^2.$$

Il faut prendre le signe supérieur, et l'on a

$$p^4 - y^2 = 2^{4a-2} q^4.$$

De là

$$p^2 \pm y = 2r^4, \quad p^2 \mp y = 2^{4a-3} s^4,$$

en prenant

$$q = rs, \quad D(r,s) = 1.$$

L'addition donne

$$p^2 = r^4 + (2^{a-1} s)^4;$$

donc, etc.

Remarque. — Euler, dans son *Algèbre*, démontre l'impossibilité de l'équation $x^4 + y^4 = z^2$ par une méthode dite de Fermat et qui consiste à montrer qu'une solution en nombres positifs conduirait à une autre solution en nombres plus petits, et ainsi de suite à l'infini, ce qui implique contradiction. Les transformations sont basées sur la réso-

lution de l'équation

$$x^2+y^2=z^2.$$

Il est vrai qu'elle est toujours possible, puisque

$$(p^2-q^2)^2+(2pq)^2=(p^2+q^2)^2$$

est une identité, mais cela suppose que x, y, z ne sont pas soumis à certaines restrictions. Ainsi quand on aura prouvé, comme plus haut, qu'une seule des inconnues est paire, et que cette inconnue paire x est double d'un impair, l'impossibilité sera démontrée, car alors

$$x^2=z^2-y^2$$

n'est pas même une congruence pour le module 8, le premier membre ayant la forme $8k+4$ et le second la forme $8f$.

Puisque dans la méthode dite de Fermat on part d'une solution supposée existante et en nombres entiers, il est impossible que les solutions en nombres décroissants se prolongent à l'infini. Quand un examen plus approfondi fera voir le point où les transformations cessent d'être praticables, l'impossibilité sera prouvée si les transformations employées sont seules possibles. Dans le cas présent, la méthode de Fermat revient à la précédente qu'on peut nommer méthode de *non-congruence* (*V.* l'*Algèbre d'Euler*, ch. 14).

Une conséquence de l'impossibilité de $x^4+y^4=z^2$ est celle de $x^4+y^4=u^4$. Fermat a avancé que pour $m>2$ l'équation $x^m+y^m=z^m$ est impossible. Cette proposition n'a pas encore été démontrée généralement. Les cas les plus simples peuvent s'établir par la méthode de non-congruence, qui consiste à établir qu'il n'y a pas congruence pour un module convenablement choisi et par suite qu'il n'y a pas égalité.

Pour le cas de l'exposant pair, on peut généraliser et ramener l'impossibilité de l'équation

$$x^{2m}+y^{2m}=z^2$$

à celle de

$$p^m+q^m=r^m,$$

le nombre m étant impair.

Théorème de Fermat. — Ses conséquences.

40. La proposition suivante, due à Fermat, est remarquable par ses nombreuses conséquences.

Théorème. — ***Pour le nombre premier* P *on a, quand* a *n'est pas divisible par* P, $a^{P-1} \equiv 1$ mod. P.**

Démonstration. — **1° Dans le développement de $(a+1)^P$ tous les termes, sauf le premier et le dernier, sont multiples de P, parce que $\frac{P(P-1)\ldots(P-i+1)}{1.2\ldots i}$ est multiple de P. On aura donc**

$$(a+1)^P \equiv a^P + 1 \quad \text{mod. P},$$

ou

$$(a+1)^P - (a+1) \equiv a^P - a \quad \text{mod. P}.$$

Or pour $a = 1$ le second membre $1^P - 1$ est divisible par P, donc $2^P - 2$ l'est aussi; puis en posant $a = 2$, on aura $3^P - 3$ divisible par P, et ainsi de suite.

On a généralement $a^P - a = a(a^{P-1} - 1)$ divisible par P, et comme a ne l'est pas, ce sera $a^{P-1} - 1$; on a donc $a^{P-1} \equiv 1$ mod. P.

2° La formule du polynôme donne semblablement

$$(a + b + c + d\ldots)^P \equiv a^P + b^P + c^P + d^P + \ldots \quad \text{mod. P}.$$

Faisant $a = b = c = d \ldots = 1$, le nombre des termes étant k, on aura

$$k^P \equiv k, \quad \text{ou} \quad k^{P-1} \equiv 1 \quad \text{mod. P}.$$

Ces deux démonstrations sont d'Euler; en voici une troisième de Gauss.

3° Prenez les multiples de a,

$$a, \quad 2a, \quad 3a, \ldots, \quad (P-1)a,$$

divisez-les par P, et soient

$$r_1, \quad r_2, \quad r_3, \ldots, \quad r_{p-1},$$

les restes, ils seront différents et formeront à l'ordre près la suite

$$1, \; 2, \; 3, \ldots, \; P-1.$$

Car, si l'on avait $ia = Pq + r_i$, $ja = Pq' + r_j$ et $r_i = r_j$, il viendrait $(i-j)a$ divisible par P, ce qui est impossible; les restes sont donc différents.

Si l'on multiplie membre à membre les $P-1$ équations qui se tirent de $ia = Pq + r_i$ en donnant à i les valeurs $1, 2, 3 \ldots P-1$, on trouvera, en négligeant les multiples de P dans le produit des seconds membres,

$$1.2.3\ldots(P-1)a^{P-1} \equiv 1.2.3\ldots P-1 \quad \text{mod.} P,$$

et par suite $a^{P-1} \equiv 1$ mod. P, parce que $1.2.3\ldots(P-1)$ n'est pas divisible par P.

Remarque. — Les restes r et $P-r$ sont dits complémentaires; ils ne peuvent se présenter dans la suite

$$r_1,\ r_2,\ r_3,\ \ldots,\ r_{\frac{P-1}{2}}$$

car $ia \equiv r$ et $ja \equiv P-r$ donnent $(i+j)a \equiv 0$ mod. P ou $i+j$ multiple de P, ce qui est impossible quand i et j appartiennent à la suite $1, 2, 3, \ldots, \frac{P-1}{2}$.

41. Cette dernière démonstration s'applique à la proposition suivante, généralisation du théorème de Fermat.

THÉORÈME. — *Lorsque* a *est premier à* m, *on a*

$$a^{\varphi(m)} \equiv 1 \quad \text{mod.} m.$$

Démonstration. — Soient $1, \alpha, \beta, \ldots, \lambda, \mu$, les $\varphi(m)$ nombres inférieurs et premiers à m; les restes des produits

$$a,\ \alpha a,\ \beta a, \ldots,\ \lambda a,\ \mu a$$

divisés par m seront différents et formeront, à l'ordre près, la suite $1, \alpha, \ldots, \mu$, d'où l'on conclura, comme plus haut, que l'on a

$$a^{\varphi(m)} \equiv 1 \quad \text{mod. } m.$$

Cette généralisation est d'Euler.

Il est utile de remarquer le cas particulier suivant :

Pour $m = P^\alpha$ on a, quand P ne divise pas a,

$$a^{P^{\alpha-1}(P-1)} \equiv 1 \quad \text{mod. } P^\alpha.$$

Si $\alpha = 1$, on retombe sur le théorème de Fermat.

Remarque. — Comme $a^{P-1}-1=\left(a^{\frac{P-1}{2}}-1\right)\left(a^{\frac{P-1}{2}}+1\right)$, on a l'une des congruences

$$a^{\frac{P-1}{2}}\equiv 1,\quad a^{\frac{P-1}{2}}\equiv -1 \mod. P.$$

La suite montrera l'utilité d'une règle pratique pour savoir si le reste de $a^{\frac{P-1}{2}}$ divisé par P est $+1$ ou -1.

42. Théorème. — *Si parmi les restes des nombres*

$$a,\ 2a,\ 3a,\ldots \left(\frac{P-1}{2}\right)a,$$

divisés par P, *il y en a* n *qui surpassent* $\frac{P-1}{2}$, *on aura*

$$a^{\frac{P-1}{2}}\equiv(-1)^n \quad \mod. P.$$

Démonstration. — Soient les restes $r_1, r_2, \ldots r_{\frac{P-1}{2}}$; comme ils ne contiennent pas de restes complémentaires, en remplaçant $r_i>\frac{P-1}{2}$ par $P-(P-r_i)=P-\rho_i$, on aura

$$\rho_i<\frac{P-1}{2},$$

de sorte que les nombres $r_\alpha, r_\beta, r_\gamma, \ldots$, non supérieurs à $\frac{P-1}{2}$, et les nombres $\rho_1, \rho_2, \ldots, \rho_n$ inférieurs à $\frac{P-1}{2}$: seront à l'ordre près

$$1,\ 2,\ 3,\ldots,\ \frac{P-1}{2};$$

on aura donc

$$r_1 . r_2 . r_3 \ldots r_{\frac{P-1}{2}} \equiv 1.2.3 \ \ldots \frac{P-1}{2}(-1)^n \mod. P.$$

Mais comme on a

$$1.2.3\ldots\frac{P-1}{2}\cdot a^{\frac{P-1}{2}}\equiv r_1 . r_2 . r_3 \ldots r_{\frac{P-1}{2}} \quad \mod. P,$$

il en résultera

$$a^{\frac{P-1}{2}} \equiv (-1)^n, \quad \text{mod. P.}$$

Cette proposition est de Gauss.

Théorème. — *Pour $a=2$, on a*

$$n = \frac{P-1}{2} - E\left(\frac{P-1}{4}\right),$$

et par suite

$$2^{\frac{P-1}{2}} \equiv 1, \quad \text{mod. P}, \quad \textit{pour} \quad P = 8K \pm 1,$$
$$2^{\frac{P-1}{2}} \equiv 1, \quad \text{mod. P}, \quad \textit{pour} \quad P = 8K \pm 3,$$

ce qui revient à

$$2^{\frac{P-1}{2}} \equiv (-1)^{\frac{P^2-1}{8}}, \quad \text{mod. P.}$$

Si l'on pose $P = 4q \pm 1$, *on a encore*

$$2^{\frac{P-1}{2}} \equiv (-1)^q, \quad \text{mod. P.}$$

Démonstration. — Les produits a, $2a$, $3a$, ..., $\frac{P-1}{2}a$ sont, pour $a=2$, égaux à 2, 4, 6, ..., P — 1. Les restes r_1, r_2, ... ne diffèrent pas de ces produits et vont en croissant; le premier reste $2x$ qui surpasse $\frac{P-1}{2}$ est donné par l'inégalité

$$2x > \frac{P-1}{2} \quad \text{ou} \quad x > \frac{P-1}{4},$$

le nombre des restes plus grand que $\frac{P-1}{2}$ est donc

$$n = \frac{P-1}{2} - E\left(\frac{P-1}{4}\right).$$

Si $P = 4q+1$,

$$n = 2q - q = q;$$

$P = 4q - 1$ donne

$$n = 2q - 1 - (q-1) = q;$$

on a donc, pour $P = 4q \pm 1$,

$$2^{\frac{P-1}{2}} \equiv (-1)^q, \quad \text{mod. P.}$$

Comme $\frac{P^2-1}{8} = 2q^2 \pm q$ et $2q^2 - q = 2(q^2 - q) + q$, on aura

$$q \equiv \frac{P^2-1}{8} \text{ mod. } 2 \quad \text{et} \quad 2^{\frac{P-1}{2}} \equiv (-1)^{\frac{P^2-1}{8}}, \quad \text{mod. P.}$$

Remarque. — C'est dans la théorie de l'équation $x^2 = a + Py$ qu'il convient de transformer la valeur de n qui donne

$$a^{\frac{P-1}{2}} \equiv (-1)^n, \quad \text{mod. P.}$$

Il suffit de dire ici qu'en supposant a positif et inférieur à P, la vraie valeur de n, ou le nombre des restes de $a, 2a, 3a, \ldots, \left(\frac{P-1}{2}\right) a$ supérieurs à $\frac{P-1}{2}$, est donnée par la proposition qui suit :

THÉORÈME. — *Si le nombre positif $a < P$ est égal à $2\alpha + r$, r étant* o *ou* 1, *selon que a est pair ou impair, on aura*

$$a^{\frac{P-1}{2}} \equiv (-1)^n,$$

$$n = -E\left(\frac{P}{2a}\right) + E\left(\frac{2P}{2a}\right) - E\left(\frac{3P}{2a}\right) + \ldots + E\left(\frac{2\alpha P}{2a}\right).$$

Démonstration. — Elle est analogue à celle donnée pour $a = 2$.

Cas particuliers. — Pour $a = 2$, on a $\alpha = 1$, $r = 0$, et

$$n = -E\left(\frac{P}{4}\right) + E\left(\frac{P}{2}\right) = \frac{P-1}{2} - E\left(\frac{P}{4}\right),$$

ce qui s'accorde avec ce qui précède, car $E\left(\frac{P}{4}\right) = E\left(\frac{P-1}{4}\right)$.

Pour $a = 3$, on a $\alpha = 1$, $r = 1$, et

$$n = E\left(\frac{P}{3}\right) - E\left(\frac{P}{6}\right).$$

Pour $a=5$, on a $\alpha=2$, $r=1$, et

$$n=-E\left(\frac{P}{10}\right)+E\left(\frac{2P}{10}\right)-E\left(\frac{3P}{10}\right)+E\left(\frac{4P}{10}\right)$$
$$=E\left(\frac{P}{5}\right)+E\left(\frac{2P}{5}\right)-\left[E\left(\frac{P}{10}\right)+E\left(\frac{3P}{10}\right)\right],$$

et ainsi de suite.

43. Voici un théorème qui fait connaître les restes des sommes

$$S_m=1^m+2^m+3^m+\ldots+(P-1)^m.$$

THÉORÈME.—*Lorsque m est multiple de* P—1, *on a* $S_m \equiv P-1$ mod. P *et, dans le cas contraire,* $S_m \equiv 0$ mod. P.

Démonstration.—Pour le premier cas, on a $a^{K(P-1)} \equiv 1$ et, comme la somme S_m a a $P-1$ termes congrus à 1, on aura

$$S_m \equiv P-1, \quad \text{mod.}\,P.$$

Pour le second cas, on considère les équations

$$2\Sigma x = x(x+1)$$
$$3\Sigma x(x+1) = x(x+1)(x+2)$$
$$4\Sigma x(x+1)(x+2) = x(x+1)(x+2)(x+3)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(P-1)\Sigma x(x+1)\ldots(x+P-3) = x(x+1)\ldots(x+P-2)$$
$$P\Sigma x(x+1)\ldots(x+P-2) = x(x+1)\ldots(x+P-1).$$

Si l'on pose

$$x=P-1, \quad \text{ou} \quad x+1=P,$$

la première équation donne

$$\Sigma(P-1)=S_1 \equiv 0, \quad \text{mod.}\,P,$$

puis la seconde, qui revient à

$$3\Sigma x^2+3\Sigma x = x(x+1)(x+2),$$

donne

$$\Sigma x^2=\Sigma(P-1)^2=S_2,$$

divisible par P, puisque Σx l'est aussi, de même que le deuxième

membre; et ainsi de suite jusqu'à l'avant-dernière équation qui donne

$$S_{(P-2)} \equiv 0, \quad \text{mod. P.}$$

En général, $m = q(P-1) + r$ donne

$$a^m \equiv a^r \quad \text{et} \quad S_m \equiv S_r, \ \text{mod. P.}$$

Remarque. — Les équations précédentes pourraient faire connaître les valeurs exactes des sommes. On a

$$\Sigma x = \frac{x(x+1)}{2}, \quad \Sigma x^2 = \frac{x(x+1)(2x+1)}{1.2.3}, \quad \Sigma x^3 = \left[\frac{x(x+1)}{2}\right]^2,$$

et ainsi de suite, les formules se compliquant de plus en plus.

Théorème de Wilson.

44. L'équation

$$P\Sigma x(x+1)(x+2)\ldots(x+P-2) = x(x+1)\ldots(x+P-1)$$

conduit à un théorème remarquable que l'on nomme *Théorème de Wilson*, du nom de celui qui l'a énoncé le premier. Il convient exclusivement aux nombres premiers, mais la longueur des calculs empêche qu'on puisse s'en servir pour voir si un grand nombre est premier ou non.

THÉORÈME DE WILSON. — *On a, pour tout nombre premier* P,

$$1 + 1.2.3\ldots(P-1) \equiv 0, \quad \text{mod. P.}$$

Démonstration. — Si, dans l'équation

$$P\Sigma x(x+1)(x+2)\ldots(x+P-2) = x(x+1)(x+2)\ldots(x+P-1),$$

on fait $x = P-1$, chaque membre sera divisible par P. La division étant faite, si l'on néglige dans le premier membre les sommes multiples de P, et que dans le second

$$(P-1)(P+1)(P+2)\ldots(P+P-2),$$

on néglige P dans les facteurs $P-1$, $P+2, \ldots$, ce qui le réduit à

$1.2.3\ldots(P-2)(P-1)$, on aura

$$-1 \equiv 1.2.3\ldots(P-1), \quad \text{mod. } P,$$

ce qui revient à l'énoncé.

Théorème. — *Le nombre p n'étant pas premier, on a*

$$1.2.3\ldots(p-1) \equiv 0, \quad \text{mod. } p,$$

excepté pour $p = 4$ *qui donne* $1.2.3 \equiv 2$, mod. 4.

Démonstration. — 1° Si $p = qr$, les nombres q et r étant inégaux, se trouvent dans la suite $1, 2, 3, \ldots, p-1$; le produit $1.2.3\ldots(p-1)$ est donc divisible par p. 2° Soit $p = q^2$, si $p-1$ égale ou surpasse $2q$, on aura $1.2.3\ldots p-1$ divisible par $q.2q = 2q^2 = 2p$, et par conséquent divisible par p; comme $p - 1 = q^2 - 1$, la condition $q^2 - 1 > 2q$ revient à $(q-1)^2 > 2$ ou $q > 1 + \sqrt{2} > 2$.

Théorème. — *La congruence à module premier* P

$$1 + 1.2.3\ldots(P-1) \equiv 0, \quad \text{mod. } P,$$

revient à

$$\left[1.2.3\ldots\left(\frac{P-1}{2}\right)\right]^2 + (-1)^{\frac{P+1}{2}} \equiv 0, \quad \text{mod. } P,$$

savoir, pour $P \equiv 1$, mod. 4,

$$\left[1.2.3\ldots\left(\frac{P-1}{2}\right)\right]^2 + 1 \equiv 0, \quad \text{mod. } P,$$

et, pour $P \equiv 3$, mod. 4,

$$\left[1.2.3\ldots\left(\frac{P-1}{2}\right)\right]^2 - 1$$

$$= \left[1.2.3\ldots\left(\frac{P-1}{2}\right) - 1\right]\left[1.2.3\ldots\left(\frac{P-1}{2}\right) + 1\right] \equiv 0, \quad \text{mod. } P.$$

Démonstration. — Cela suit de ce que l'on a $i(P-i) \equiv -i^2$, mod. P, et de ce que l'on prend pour i les nombres $1, 2, 3, \ldots, \frac{P-1}{2}$.

Remarque. — Pour $P \equiv 3$, mod. 4, l'un des nombres

$$\left[1.2.3\ldots\left(\frac{P-1}{2}\right)\right]-1, \quad \left[1.2.3\ldots\left(\frac{P-1}{2}\right)\right]+1,$$

est divisible par P; il n'est pas facile de dire à priori lequel de ces deux nombres est multiple de P.

45. Théorème. — *Le nombre n étant égal ou inférieur à* P, *la fonction entière*

$$f(x) = ax^n + bx^{n-1} + \ldots + fx + g$$

ne peut être rendue divisible par P, *nombre premier, par plus de n nombres inférieurs à* P.

N. B. On suppose le premier coefficient non multiple de P.

Démonstration. — 1° Cela a été prouvé pour $ax+b$; il n'y a qu'un nombre inférieur à P qui rende $ax+b$ divisible par P. 2° Soit ax^2+bx+c; si un premier nombre $x=\alpha$ donne $a\alpha^2+b\alpha+c$ multiple de P, pour d'autres valeurs de x qui rendent ax^2+bx+c multiple de P,

$$ax^2+bx+c-(a\alpha^2+b\alpha+c) = (x-\alpha)[a(x+\alpha)+b]$$

sera aussi multiple de P. Or aucune valeur de $x < P$, et autre que α, ne rend $x-\alpha$ multiple de P; c'est donc $a(x+\alpha)+b$ qui doit l'être, ce qui ne peut arriver que pour une seule valeur de x inférieure à P. Ainsi il n'y a pas plus de deux valeurs de x inférieures à P qui rendent ax^2+bx+c multiple de P. 3° On prouve de même qu'il y a au plus trois valeurs de x inférieures à P qui rendent

$$ax^3+bx^2+cx+d$$

multiple de P. Et ainsi de suite.

Théorème. — *La fonction*

$$x^{P-1}-1 = (x^m-1)(x^{(n-1)m}+x^{(n-2)m}+\ldots x^m+1),$$

où l'on suppose $P-1=m.n$, *est rendue divisible par* P *en mettant pour x les mn nombres*

$$1,\ 2,\ 3,\ldots,\ (P-1)$$

inférieurs à P. *De ces nombres, m rendent* x^m-1 *divisible par* P, *et les* $(n-1)m$ *autres rendent le second facteur*

$$x^{(n-1)m}+x^{(n-2)m}+\ldots+x^{2m}+x^m+1$$

divisible par P, *nombre premier.*

Démonstration. — Il suit du théorème de Fermat que

$$x^{P-1} - 1 = x^{mn} - 1$$

est rendu divisible par P en y faisant $x = 1, 2, 3, \ldots, P-1$. Tous ces nombres rendent

$$(x^m - 1)\left[x^{(n-1)m} + x^{(n-2)m} + \ldots + x^m + 1\right]$$

divisible par P. Si le facteur $x^m - 1$ n'était rendu divisible par P que par $m - \delta$ valeurs de x inférieures à P, il faudrait que la fonction

$$x^{(n-1)m} + \ldots + x^m + 1$$

fût rendue divisible par P par $mn - (m - \delta) = m(n-1) + \delta$ valeurs de x inférieures à P, ce qui a été démontré impossible. Il faut donc admettre que m nombres pris parmi $1, 2, 3, \ldots, P-1$ rendent $x^m - 1$ divisible par P.

Généralement si l'on a

$$x^{P-1} - 1 = f(x) \cdot f_1(x),$$

$f(x)$ étant de degré k et $f_1(x)$ de degré $P - 1 - k$, la fonction $f(x)$ sera rendue divisible par P par k valeurs de x inférieures à P, et $f_1(x)$ le sera par $P - 1 - k$ valeurs.

CHAPITRE VII.

RESTES DES NOMBRES EN PROGRESSION GÉOMÉTRIQUE. — THÉORIE DES LOGARITHMES MODULAIRES OU POUR UN MODULE DONNÉ. — TABLES OU *CANON ARITHMETICUS* DE JACOBI.

46. On sait que, le nombre a étant premier à m, il en résulte

$$a^{\varphi(m)} \equiv 1, \quad \text{mod.}\, m,$$

d'où

$$a^{k\varphi(m)} \equiv 1, \quad \text{mod.}\, m,$$

quel que soit l'entier positif k; d'après cela, pour abréger les énoncés des propositions, on admet les définitions suivantes :

I. Quand a^e est la moindre puissance de a, autre que a^0, qui soit congrue à l'unité pour le module m, on dit que le nombre *a appartient* à l'exposant e pour le module m.

II. Les restes de $1, a, a^2, \ldots, a^{e-1}$ divisés par m composent la *période* du nombre a pour le module m.

THÉORÈME. — *Les termes de la période du nombre a, qui appartient à l'exposant e, pour le module m, sont inégaux et en nombre e diviseur de* $\varphi(m)$.

Démonstration. — Par hypothèse on a $a^e \equiv 1$, mod. m, et pour des exposants α, β moindres que e on ne saurait avoir $a^\alpha \equiv 1$, $a^\beta \equiv 1$, mod. m. On ne pourra pas non plus avoir $a^\beta \equiv a^\alpha$, mod. m, car il en résulterait $a^{\alpha-\beta} \equiv 1$, mod. m, ce qui est impossible, $\alpha - \beta$ étant inférieur à e.

Les restes de la suite

$$1, \quad a, \quad a^2, \quad a^3, \ldots, \quad a^{e-1}$$

étant inégaux, il en est de même de ceux des nombres

$$a^e, \quad a^{e+1}, \quad a^{e+2}, \ldots, \quad a^{2e-1},$$

qui reviennent à ceux de la suite

$$1, \quad a, \quad a^2, \ldots, \quad a^{e-1},$$

et, en général, de $a^e \equiv 1$, mod. m, on tire

$$a^r \equiv a^{ke+r}, \quad \text{mod. } m;$$

ce qui montre que les restes des termes de la progression indéfiniment prolongée se reproduisent périodiquement. Les termes

$$a^e, \quad a^{2e}, \quad a^{3e}, \ldots, \quad a^{ke},$$

étant les seuls congrus à 1 pour le module m, puisque $a^{\varphi(m)}$ l'est aussi, il est nécessaire que $\varphi(m)$ soit multiple de e, ou autrement que e soit diviseur de $\varphi(m)$.

Seconde démonstration. — Si l'on établissait, comme le fait Euler, que l'exposant auquel appartient a pour le module m est diviseur de $\varphi(m)$, comme on aurait

$$\varphi(m) = ke, \quad a^e \equiv 1, \quad \text{mod. } m,$$

il en résulterait

$$a^{\varphi(m)} \equiv 1, \quad \text{mod. } m.$$

Voici la démonstration d'Euler :

Les restes de

(1) $$1, \quad a, \quad a^2, \ldots, \quad a^{e-1},$$

ou les termes de la période de a, sont différents et premiers à m. Si l'on n'a pas $\varphi(m) = e$, soit b un nombre inférieur et premier à m et de plus non compris dans la suite (1); on formera la suite

(2) $$b, \quad ba, \quad ba^2, \ldots, \quad ba^{e-1};$$

les restes de ces nombres seront tous différents entre eux, puisque $ba^\alpha \equiv ba^\beta$, mod. m, supposerait que l'on a $a^\alpha \equiv a^\beta$, mod. m. Ils seront aussi différents des nombres de la suite (1), puisqu'en supposant $ba^\alpha \equiv a^\beta$, mod. m, il en résulterait pour $\beta > \alpha$,

$$b \equiv a^{\beta - \alpha}, \quad \text{mod. } m,$$

ce qui est contre l'hypothèse. Pour $\alpha > \beta$, en multipliant par $a^{e-\alpha}$,

il viendrait

$$ba^e \equiv a^{\beta+e-\alpha} \quad \text{ou} \quad b \equiv a^{e-(\alpha-\beta)}, \quad \text{mod. } m,$$

contrairement à l'hypothèse.

Si l'on n'a pas $\varphi(m) = 2e$, outre les $2e$ nombres des séries (1), (2), il y en a d'autres encore inférieurs et premiers à m. Soit c un tel nombre, on montrera de même que les restes de la suite

$$(3) \qquad c, \quad ca, \quad ca^2, \ldots, \quad ca^{e-1}$$

sont premiers à m, différents entre eux et des restes des suites (1), (2), de sorte que l'on aura $3e$ nombres inférieurs et premiers à m. En continuant de même, on trouvera que l'on doit en avoir $\varphi(m) = ke$, car supposer que $\varphi(m) = ke + r$, c'est supposer par là même que $\varphi(m)$ est au moins égal à $(k+1)e$.

Exemple. — Soit $m = 31$, le nombre 2 appartient à l'exposant 5; de sa période

(1)	1,	2,	4,	8,	16,

on tire

(2)	3,	6,	12,	24,	17,
(3)	5,	10,	20,	9,	18,
(4)	7,	14,	28,	25,	19,
(5)	11,	22,	13,	26,	21,
(6)	15,	30,	29,	27,	23.

Au moyen de (1) on a obtenu tous les autres nombres inférieurs à 31 dans l'ordre particulier indiqué par les suites (2), (3), (4), (5), (6).

47. Il se présente ici plusieurs questions. Le nombre d étant diviseur de $\varphi(m)$, y a-t-il des nombres appartenant à l'exposant d? Combien y en a-t-il (on les suppose inférieurs au module)? Comment peut-on trouver ces nombres?

Pour résoudre ces questions, il convient d'examiner séparément les différentes formes du module.

Du module 2^m.

Les nombres premiers à 2^m sont les nombres impairs; comme ils ont nécessairement une des formes $4k+1$, $4k-1$, en mettant en

évidence la plus haute puissance de 2 qui divise k, on peut poser

$$i = \pm 1 + 2^\alpha a;$$

dans cette formule les lettres a, i représentent des nombres impairs, l'exposant α, qui est au moins 2, peut être pair ou impair. Sous cette forme, on voit de suite à quel exposant appartient le nombre i.

Le nombre 1, qui n'est pas contenu dans cette formule, appartient à l'exposant 1. Les nombres $2^m - 1$, $2^{m-1} \pm 1$ qui y sont contenus appartiennent à l'exposant 2. En général, on a cette proposition :

Théorème. — *Le nombre impair $i = \pm 1 + 2^\alpha a$, où a est impair, appartient à l'exposant $2^{m-\alpha}$.*

Démonstration. — Si l'on cherche quelle est la plus haute puissance de 2 qui peut diviser $i^n - 1$, le nombre n étant pair ou impair, en mettant n sous la forme $n = 2^\beta b$, le nombre b étant impair, on a d'abord

$$(\pm 1 + 2^\alpha a)^b = \pm 1 + b.2^\alpha.a \pm \frac{b.b-1}{1.2} 2^{2\alpha} a^2 + \ldots.$$

Comme à partir du troisième terme l'exposant de la plus haute puissance de 2 qui divise chaque terme surpasse α, on aura

$$(\pm 1 + 2^\alpha a)^b = \pm 1 + 2^\alpha c,$$

le nombre c étant impair. Si l'on élève maintenant à la puissance 2^β, comme l'on a

$$(\pm 1 + 2^\alpha c)^2 = 1 + 2^{\alpha+1} c\,(2^{\alpha-1} c \pm 1) = 1 + 2^{\alpha+1} d,$$

le nombre d étant impair, on aura, par suite d'élévation successive au carré,

$$(\pm 1 + 2^\alpha c)^{2^\beta} = 1 + 2^{\alpha+\beta} f,$$

f étant impair; par suite,

$$(\pm 1 + 2^\alpha a)^{2^\beta b} = 1 + 2^{\alpha+\beta} g,$$

g étant impair.

Ainsi, quel que soit b, le nombre β restant le même, $2^{\alpha+\beta}$ est la plus haute puissance de 2 qui divise $i^{2^\beta b} - 1$.

Si l'on fait $b = 1$ et $\alpha + \beta = m$, d'où $\beta = m - \alpha$, on verra i appartient à l'exposant $2^{m-\alpha}$. On a

$$\varphi(2^m) = 2^{m-1}, \quad \frac{1}{2}\varphi(2^m) = 2^{m-2};$$

comme α est au moins 2, l'exposant est non-seulement diviseur de $\varphi(2^m)$, comme il a été prouvé, mais il l'est même de $\frac{1}{2}\varphi(2^m)$. Ce n'est que pour les modules 2 et 4 qu'il faut s'élever jusqu'à l'exposant $\varphi(2^m)$.

Pour le module 2, le nombre 1 appartient à l'exposant 1, diviseur de $\varphi(2) = 1$.

Pour le module $2^2 = 4$, le nombre 1 appartient encore à l'exposant 1, mais 3 appartient à l'exposant $2 = \varphi(4)$.

Pour le module $2^3 = 8$, le nombre 1 appartient à l'exposant 1, les nombres 3, 5 et 7 appartiennent à l'exposant $2 = \frac{1}{2}\varphi(2^3)$.

Quand on a trouvé la moitié des termes de la période du nombre i, l'autre moitié s'en déduit par la proposition suivante :

Théorème. — *Quand on a trouvé la première moitié de la période, en augmentant ou diminuant les termes de 2^{m-1}, moitié du module, on a les termes de la seconde moitié.*

Démonstration. — Si le nombre i appartient à l'exposant pair $2\alpha > 2$, comme $i^{2\alpha} - 1 = (i^\alpha - 1)(i^\alpha + 1)$, α étant pair, le deuxième facteur est divisible par 2 et non par 4; $i^\alpha - 1$, qui ne peut être divisible par 2^m, l'est donc par 2^{m-1}, et l'on a

$$i^\alpha = 1 + 2^{m-1}a = 1 + 2^{m-1} + 2^m.k;$$

le nombre a étant impair, multipliant par $i^r = 2k' + 1$, il vient

$$i^{\alpha+r} = i^r + 2^{m-1} + 2^m k''.$$

Remarque. — Si l'on avait $i^r > 2^{m-1}$, comme $2^m = 2^{m-1} + 2^{m-1}$, on ferait

$$i^{\alpha+r} = i^r - 2^{m-1} + 2^m(k'' + 1),$$

c'est-à-dire qu'il faut, pour avoir le reste de $i^{\alpha+r}$, diminuer ou augmenter de 2^{m-1} celui de i^r.

48. Le plus haut exposant auquel puisse appartenir un nombre impair pour le module $2^m > 4$ est donc 2^{m-2}. Cela arrive pour les nombres $\pm 1 + 4(2k+1)$, ou $8k+3$, $8k+5$.

Dans ce cas la période contient 2^{m-2} nombres impairs, c'est-à-dire la moitié des nombres impairs inférieurs à 2^m. Au-dessous de 2^m, il y a 2^{m-1} nombres impairs partagés en quatre classes :

1° Les nombres $8k+1$, au nombre de 2^{m-3}.
2° Les nombres $8k+3$ id.
3° Les nombres $8k+5$ id.
4° Les nombres $8k+7$ id.

La période d'un nombre $8k+3$ ou $8k+5$ donne comme restes des puissances paires les nombres $8k+1$.

La période d'un nombre $8k+3$ donne les nombres $8k+3$ comme restes des puissances impaires.

La période d'un nombre $8k+5$ donne les nombres $8k+5$ comme restes des puissances impaires.

On ne trouve jamais les restes de la forme $8k+7$.

49. Quand on a calculé la période du nombre 3 ou 5 pour un module 2^m, on peut en déduire la solution de diverses questions.

Prenons pour exemple le module 32 ; le plus haut exposant auquel puisse appartenir le nombre impair 3 est $8 = \frac{1}{4}32$. La période aura 8 termes

$$1,\ 3,\ 9,\ 27\ :\ 17,\ 19,\ 25,\ 11;$$

comme on le voit,

$$17 = 1+16,\quad 19 = 3+16,\quad 25 = 9+16,\quad 11 = 27+16-32.$$

Si l'on veut rendre $x^4 - a$ divisible par 32, il faut d'abord que a ait la forme $8k+1$. Soit $a = 17$, en posant $x \equiv 3^y$, $a = 17 \equiv 3^\alpha$, il vient

$$3^{4y} - 3^\alpha = 3^\alpha(3^{4y-\alpha} - 1) = 32z.$$

Cette équation ne peut être satisfaite qu'en posant $4y - \alpha = 8t$. Or ici $\alpha = 4$, donc $y = 1 + 2t$, $y = 1, 3, 5, 7, \ldots$ donnent

$$x = 3,\ 27,\ 19,\ 25,$$

qui peuvent être pris avec le signe -1 ; il y a donc 8 nombres inférieurs à 32 qui rendent $x^4 - 17$ divisible par 32, comme on le vérifie facilement.

Pour rendre $x^3 - a$ divisible par 32, si a est de la forme $8k+3$, par exemple 19, il se trouvera parmi les restes, on aura

$$19 \equiv 3^5.$$

Soit $x \equiv 3^y$, mod. 32, on aura

$$3^{3y} - 3^5 = 3^5(3^{3y-5} - 1)$$

divisible par 32; il faut avoir $3y - 5$ divisible par 8, ou bien encore $y+1$ divisible par 8, $y = 8t - 1$, de là $y = 7$, $x = 11$. Ainsi, pour rendre $x^3 - 19$ divisible par 32, il faut prendre $x = 11$.

Si a avait été de la forme $8k+5$, il n'aurait pas été compris dans la période, on aurait fait $x \equiv -y$, de là

$$y^3 \equiv -a, \quad \text{mod. } 32.$$

Soit $a = 13$, comme $32 - 13 = 19$, on aurait eu $y^3 \equiv 19$. On a, comme on l'a vu, $y = 11$, donc

$$x = 32 - 11 = 21.$$

On voit par ces exemples l'utilité d'une Table qui donnerait les restes de la période du nombre 3, pour le module 2^m, et celle d'une seconde Table qui pour un reste donné ferait connaître l'exposant de 3. Autrement, en posant

$$a \equiv 3^\alpha, \quad \text{mod. } 2^m,$$

la première Table donnerait a connaissant α, et la seconde α connaissant a.

Voici pour le module $128 = 2^7$ la disposition des Tables d'après Jacobi :

$$m = 128 = 2^7, \qquad \frac{m}{4} = 32.$$

A. *Nombres* (correspondant aux *Indices*).

I.	0	1	2	3	4	5	6	7	8	9
		3	9	27	47	13	39	11	33	29
1	41	5	15	45	7	21	63	61	55	37
2	17	51	25	53	31	35	23	59	49	19
3	57	43	1							

B. *Indices* (correspondant aux *Nombres*).

N.	1	3	5	7	9
	32	1	11	14	2
1	7	5	12	20	29
2	15	26	22	3	9
3	24	8	25	19	6
4	10	31	13	4	28
5	21	23	18	30	27
6	17	16			

Pour la Table A, il faut remarquer que dans la période de 3 les restes qui surpassent la moitié du module 128 ont été remplacés par leur complément. On a $3^4 = 81$ et $81 > 64$, ce n'est pas 81, mais c'est $128 - 81 = 47$ que l'on a inscrit sous l'indice 4. A l'indice 24 on voit correspondre $31 = 3.8 + 7$; un tel reste n'a pu se présenter, c'est $128 - 31 = 97$ qu'il faut prendre.

Cette Table A, qui donne les nombres qui correspondent à des indices connus, étant faite, on en déduit la Table B, qui donne les indices des nombres connus. Au nombre $39 = 4.8 + 7$ on voit répondre 6, mais le reste 39 ne peut se présenter, 6 répond en réalité à $128 - 39 = 89$.

En ayant égard à cette remarque, l'emploi de la Table est très-simple.

Problème. — *Résoudre la congruence* $x^4 \equiv 73$, mod. 128, *ou l'équation* $x^4 = 73 + 128y$.

Solution. — Les valeurs de x sont égales deux à deux et de signe contraire. Si $x = \alpha$ satisfait, il en sera de même de $-\alpha$ ou $128 - \alpha$; comme α est nécessairement impair, des nombres α, $128 - \alpha$, l'un appartiendra nécessairement à l'une des formes $8k + 1$, $8k + 3$, nombres qui, pour la base 3, répondent à de certains indices. Une de ces deux valeurs doit être donnée par la Table. On a, en posant $73 = 128 - 55$,

$$73 \equiv 3^{18}, \quad \text{mod. } 128.$$

Soit $x \equiv 3^{\text{ind}\,x}$, mod. 128, il vient

$$3^{4\,\text{ind}\,x} \equiv 3^{18}, \quad \text{mod. } 128,$$

ou bien

$$3^{4\,\text{ind}\,x - 18} \equiv 1,$$

ce qui ne peut arriver que pour $4\,\text{ind}\,x - 18$, multiple de $32 = \frac{1}{4}\,128$; or cela est impossible, l'équation l'est donc aussi; mais $x^2 = 73 + 128y$ ne l'est pas. Dans ce cas, il faut poser

$$2\,\text{ind}\,x - 18 = 32y, \quad \text{ind}\,x = 9 + 16y,$$

de là

$$\text{ind}\,x = 9 \quad \text{et} \quad \text{ind}\,x = 25,$$

auxquels répondent $x = 29$ et $x = 35$.

Ainsi la congruence $x^4 \equiv 73$, mod. 128, est impossible. La con-

gruence $x^2 \equiv 73$, mod. 128, a quatre solutions ± 29, ± 35; la substitution les vérifie.

Problème. — *Résoudre la congruence* $x^7 \equiv 33$, mod. 128.

Une telle congruence, l'exposant étant impair, est toujours possible. Comme $33 = 8.4 + 1$, 33 a un indice, et l'on devra poser

$$7 \operatorname{ind} x - \operatorname{ind} 33 = 32.y;$$

comme $\operatorname{ind} 33 = 8$, on a

$$7 \operatorname{ind} x = 8 + 32y = 8(1 + 4y);$$

$y = 5$ donne

$$1 + 4y = 21 = 3.7;$$

donc

$$\operatorname{ind} x = 24,$$

et généralement

$$\operatorname{ind} x = 24 + 32z;$$

mais il suffit de prendre $\operatorname{ind} x = 24$, d'où

$$x = 128 - 31.$$

On vérifie que l'on a

$$31^2 \equiv 65, \quad 31^3 \equiv 95, \quad 31^4 \equiv 1, \quad 31^7 \equiv 95 \equiv -33;$$

donc

$$(-31)^7 \equiv 33, \quad \text{mod. } 128.$$

Problème. — *Résoudre la congruence* $x^5 \equiv 31$, mod. 128.

Le nombre 31 étant de forme $8k + 7$, on fera

$$(-x)^5 \equiv -31 \equiv 97.$$

Au nombre -31 répond 24; en posant $-x = z$, il viendra

$$5 \operatorname{ind} z - 24 = 32y,$$

ou bien

$$5 \operatorname{ind} z = 8(3 + 4y);$$

$y = 3$ donne

$$3 + 4y = 15,$$

donc

$$\operatorname{ind} z = 24,$$

d'où

$$z = -31 \quad \text{et} \quad x = 31;$$

et, en effet, on a, d'après les calculs précédents,

$$31^5 \equiv 31.$$

Sans avoir égard à ces changements de signe, on posera

$$5 \operatorname{ind} x - \operatorname{ind} 31 \equiv 0, \quad \text{mod.}\, 32,$$

de là

$$\operatorname{ind} x = 24, \quad x = 31.$$

En général, étant donnée la congruence

$$ax^n \equiv b, \quad \text{mod.}\, 2^m,$$

on en déduira

$$\operatorname{ind} a + n \operatorname{ind} x - \operatorname{ind} b \equiv 0, \quad \text{mod.}\, 2^{m-2},$$

ou bien

$$n \operatorname{ind} x = \operatorname{ind} b - \operatorname{ind} a + 2^{m-2} z.$$

Pour la possibilité, il faut que la plus haute puissance de 2, qui divise n et 2^{m-2}, divise aussi $\operatorname{ind} b - \operatorname{ind} a$.

Du module premier impair P.

50. Pour un module premier impair P, quand on a trouvé l'exposant diviseur de $P-1$ auquel appartient un nombre a plus petit que P, on prouve de diverses manières qu'il y a des nombres appartenant à l'exposant $P-1$ et qu'ils sont en nombre $\varphi(P-1)$. On prouve plus généralement que, quel que soit d diviseur de $P-1$, il y a $\varphi(d)$ nombres plus petits que P et appartenant à l'exposant d.

Si le nombre a appartient à l'exposant d, on a $a^d - 1$ multiple de P, a est donc l'un des d nombres inférieurs à P qui rendent $x^d - 1$ multiples de P. De plus, les restes, tous différents, des nombres

$$1, \quad a, \quad a^2, \ldots, \quad a^{d-1}$$

divisés par P sont les seuls nombres qui puissent rendre $x^d - 1$ multiple de P; c'est donc parmi ces restes qu'il faut chercher les autres nombres qui pourraient appartenir à l'exposant d. Pour savoir à quel exposant appartient a^i, ou, ce qui est la même chose, le reste de a^i divisé par P, il faut trouver le moindre nombre e qui donne ie, multiple de d. Comme le moindre multiple de i et d est $\frac{di}{D(d, i)}$, il faudra prendre $e = \frac{d}{D(d, i)}$. Ce nombre ne peut être égal à d que

si l'on a $D(d, i) = 1$, ou i premier à d. Comme au-dessous de d il n'y a que $\varphi(d)$ nombres premiers à d, on aura cette proposition :

THÉORÈME. — *S'il y a un nombre a qui appartienne à l'exposant d, il y en aura $\varphi(d)$ donnés par la suite*

$$a, \quad a^{\alpha}, \quad a^{\beta}, \ldots, \quad a^{\delta},$$

où les exposants $1, \alpha, \beta, \ldots, \delta$ sont tous les nombres inférieurs et premiers à d.

De là résulte encore cette proposition :

THÉORÈME. — *Il y a des nombres qui appartiennent à un diviseur quelconque d de $P-1$.*

Démonstration. — Au diviseur 1 appartient le nombre 1. Au diviseur 2 le nombre -1 ou $P-1$; si $d, d', d'', \ldots$, sont les autres diviseurs de $P-1$ auxquels appartiennent les autres nombres de la suite $1, 2, 3, \ldots, P-1$, comme tout nombre inférieur à P appartient à un certain exposant, on aura

$$\varphi(1) + \varphi(2) + \varphi(d) + \varphi(d') + \ldots = P - 1.$$

Or on a trouvé

$$\Sigma\varphi(d) = P - 1 ;$$

la somme s'étendant à tous les diviseurs de d, il est donc nécessaire qu'il y ait des nombres appartenant à tout diviseur de $P-1$, car autrement le nombre $P-1$ aurait deux valeurs inégales.

Voici un autre mode de démonstration :

THÉORÈME. — *Si les nombres a, b appartiennent à des exposants différents α et β dont l'un ne soit pas multiple de l'autre, il y aura des nombres appartenant à l'exposant $m(\alpha, \beta)$, moindre multiple de α et β, et par conséquent plus grand que chacun de ces nombres.*

Démonstration. — On décomposera $m(\alpha, \beta)$ en deux facteurs α', β' premiers entre eux, le premier diviseur de α et le second de β. La chose est toujours possible, comme on le voit, en décomposant α et β en leurs facteurs premiers ; il y a même plusieurs solutions, si un même facteur P a le même exposant dans α et β. Cela posé, comme l'on a

$$\left(a^{\frac{\alpha}{\alpha'}} \cdot b^{\frac{\beta}{\beta'}}\right)^{\alpha'\beta'} = a^{\alpha \cdot \beta'} \cdot b^{\beta \cdot \alpha'} ;$$

Si l'on avait $r = m + r'$, il viendrait

$$k^{2m+r'} \equiv k^{2m}.k^{r'} \equiv P - a,$$

ou encore

$$k^{r'} = k^{r-m} \equiv P - a, \quad \text{mod. P.}$$

Si l'on fait $2m = P - 1$, on a le cas de l'énoncé. Quant à la dernière partie, elle a été prouvée plus haut.

THÉORÈME. — *La congruence* $g^\alpha \equiv g^\beta$, mod. P, *donne*

$$\alpha \equiv \beta, \quad \text{mod. } P - 1.$$

Démonstration. — La quantité $g^\alpha - g^\beta = g^\beta(g^{\alpha-\beta} - 1)$ étant divisible par P, $g^{\alpha-\beta} - 1$ doit l'être; il faut donc que $\alpha - \beta$ soit multiple de $P - 1$.

D'après Gauss, au lieu de poser $g^\alpha \equiv a$, mod. P, on pose $g^{\text{ind}\,a} \equiv a$, mod. P. L'abréviation ind a, pour indice de a, représente un nombre entier inférieur à P. Dans les *Disquisitiones*, Gauss donne les indices des nombres premiers pour les modules inférieurs à 100. Il est bien préférable d'avoir une Table donnant les indices de tous les nombres inférieurs à P. La Table de Jacobi, *Canon arithmeticus*, est construite pour les modules inférieurs à 1000. Au lieu de calculer les nombres répondant aux indices $1, 2, 3, \ldots, P - 1$, on peut se contenter de calculer ceux qui répondent aux indices $1, 2, 3, \ldots, \frac{P-1}{2}$, car, en vertu de $g^{\frac{P-1}{2}} \equiv -1$, et de $g^{\text{ind}\,a} \equiv a$, on tire

$$g^{\text{ind}\,a \pm \frac{P-1}{2}} \equiv -a \equiv P - a, \quad \text{mod. P.}$$

Au moyen de cette Table, on en forme une autre donnant les indices des nombres. Si l'on a ceux des nombres inférieurs à $\frac{P-1}{2}$, on peut en déduire les autres, puisque $a < \frac{P-1}{2}$ donne

$$P - a > \frac{P-1}{2},$$

et que d'ailleurs de $a \equiv g^{\text{ind}\,a}$ on tire

$$P - a \equiv g^{\text{ind}\,a \pm \frac{P-1}{2}}.$$

Si, en calculant les restes de $1, g, \ldots, g^{\frac{P-1}{2}}$, on a trouvé

$$g^{\text{ind}\,a} \equiv a,$$

ind a et a étant plus petits que $\frac{P-1}{2}$, on aura par là même l'indice d'un nombre $< \frac{P-1}{2}$; mais si, ind a étant $< \frac{P-1}{2}$, on avait

$$a > \frac{P-1}{2},$$

on prendrait

$$g^{\text{ind}\,a + \frac{P-1}{2}} \equiv P - a, \quad \text{mod. P.}$$

Comme $P - a$ est plus petit que $\frac{P-1}{2}$, on obtiendra ainsi tous les indices des nombres inférieurs à $\frac{P-1}{2}$. Si l'on prolongeait la Table de Jacobi, ce qui serait fort utile, on pourrait sans inconvénient l'abréger de moitié, comme il vient d'être dit.

Gauss, dans ses *Disquisitiones*, ne donne pas la Table qui fait connaître les indices des nombres. Il montre comment la Table qui donne la réduction des fractions $\frac{a}{P}$ en fractions décimales périodiques peut faire connaître les indices des nombres pour le module P; ce moyen est ingénieux, mais long et incommode.

Un seul exemple de l'usage de ces Tables suffira ici.

Pour rendre $x^m - a$ divisible par P, on posera

$$x \equiv g^{\text{ind}\,x}, \quad a \equiv g^{\text{ind}\,a}, \quad \text{mod. P};$$

de là

$$g^{m\,\text{ind}\,x} \equiv g^{\text{ind}\,a},$$

ou bien

$$g^{m\,\text{ind}\,x - \text{ind}\,a} \equiv 1,$$

ou encore

$$m\,\text{ind}\,x - \text{ind}\,a = (P-1)y.$$

Il suffit donc de rendre $\text{ind}\,a + (P-1)y$ multiple de m, ce qu'on sait faire, quand le plus grand diviseur commun à $P - 1$ et à m divise le nombre ind a.

On pourrait remplacer le mot *indice* par *logarithme* pour le module P, et l'abréviation *ind.a* par L.*a*.

Voici pour le module $P = 61$, $P - 1 = 2^2.3.5$ la disposition de la Table de Jacobi.

$$P = 61, \qquad P - 1 = 2^2.3.5.$$

A. *Nombres.*

I.	0	1	2	3	4	5	6	7	8	9
		10	39	24	57	21	27	26	16	38
1	14	18	58	31	5	50	12	59	41	44
2	13	8	19	7	9	29	46	33	25	6
3	60	51	22	37	4	40	34	35	45	23
4	47	43	3	30	56	11	49	2	20	17
5	48	53	42	54	52	32	15	28	36	55
6	1									

B. *Indices.*

N.	0	1	2	3	4	5	6	7	8	9
		60	47	42	34	14	29	23	21	24
1	1	45	16	20	10	56	8	49	11	22
2	48	5	32	39	3	28	7	9	57	25
3	43	13	55	27	36	37	58	33	9	2
4	35	18	52	41	19	38	26	40	50	49
5	15	31	54	51	53	59	44	4	12	17
6	30									

La Table A contient la période du nombre 10, racine primitive du module 61. Dans des cases correspondantes aux indices ou exposants 1, 2, 3,... on voit les restes de 10, 10^2, 10^3,... divisés par 61. La Table A contient la période entière ou les restes de 10, 10^2, 10^3,..., 10^{60}; mais il suffit de calculer la demi-période 1, 10, 10^2,..., 10^{30}: ainsi on pourrait sans inconvénient supprimer tout ce qui est audessous de la ligne ponctuée.

La Table B donne les indices, exposants ou logarithmes modulaires des nombres 1, 2, 3,...; elle se forme au moyen de la première. Dans ces Tables, chaque ligne contient dix nombres, les unités de l'argument sont sur une première horizontale, les dizaines sur la première colonne verticale.

Voici un exemple de l'emploi de cette Table : Soit proposé de résoudre la congruence

$$x^7 \equiv 31, \quad \text{mod. } 61,$$

ou l'équation

$$x^7 = 31 + 61y.$$

Comme on peut poser $x \equiv 10^{\text{ind}\,x}$, $31 \equiv 10^{\text{ind}\,31}$, il vient

$$10^{7\,\text{ind}\,x} \equiv 10^{\text{ind}\,31}, \quad \text{mod. } 61,$$

ou

$$10^{7\,\mathrm{ind}\,x - \mathrm{ind}\,31} \equiv 1, \quad \mathrm{mod.}\,61,$$

ou encore

$$7\,\mathrm{ind}\,x - \mathrm{ind}\,31 \equiv 0, \quad \mathrm{mod.}\,60,$$

ce qui revient à

$$7\,\mathrm{ind}\,x - 13 = 60y.$$

Pour rendre $60y + 13$ divisible par 7, il suffit de faire $y = 2$; ainsi

$$\mathrm{ind}\,x = \frac{133}{7} = 19,$$

d'où

$$x = 44.$$

En général, étant donnée la congruence

$$ax^n \equiv b, \quad \mathrm{mod.}\,P,$$

on en tire

$$\mathrm{ind}\,a + n\,\mathrm{ind}\,x \equiv \mathrm{ind}\,b, \quad \mathrm{mod.}\,P - 1\,;$$

car en faisant

$$a \equiv g^{\mathrm{ind}\,a}, \quad x \equiv g^{\mathrm{ind}\,x}, \quad x^n \equiv g^{n\,\mathrm{ind}\,x}, \quad \mathrm{mod.}\,P,$$

il vient

$$g^{\mathrm{ind}\,a + n\,\mathrm{ind}\,x} \equiv g^{\mathrm{ind}\,b}, \quad \mathrm{mod.}\,P.$$

ou bien

$$g^{\mathrm{ind}\,a + n\,\mathrm{ind}\,x - \mathrm{ind}\,b} \equiv 1, \quad \mathrm{mod.}\,P,$$

ou encore

$$\mathrm{ind}\,a + n\,\mathrm{ind}\,x - \mathrm{ind}\,b \equiv 0, \quad \mathrm{mod.}\,P - 1,$$

ce qui revient à

$$n\,\mathrm{ind}\,x - (P-1)y = \mathrm{ind}\,b - \mathrm{ind}\,a.$$

Cette équation fera connaître $\mathrm{ind}\,x$, puis la Table donnera x.

Du module P^n.

82. Quand on connaît les racines primitives du module P ou les nombres appartenant à l'exposant $P - 1 = \varphi(P)$, on trouve immédiatement les nombres qui, pour le module P^n, appartiennent à l'exposant $P^{n-1}(P-1) = \varphi(P^n)$. On posera les formules

$$(a) \qquad g + Pz, \quad g' + Pz, \quad g'' + Pz, \ldots,$$

au nombre de $\varphi(P-1)$. Les nombres g, g', g'' étant les racines primitives pour le module P, ces formules contiendront toutes les racines primitives, c'est-à-dire qui appartiennent à l'exposant $P^{n-1}(P-1)=\varphi(P^n)$, mais elles en contiendront aussi de non primitives qu'on déterminera comme il suit : Pour la formule $g+Pz$, on commencera par poser

$$g^P = g + Ph + P^2 k,$$

c'est-à-dire que $g+Ph$ sera le reste de g^P divisé par P^2; ce reste fera connaître h. Dans $g+Pz < P^n$, on a

$$z=0,\ 1,\ 2,\ 3,\ldots,\ P^{n-1}-1;$$

de ces P^{n-1} valeurs de z il faut exclure celles qui ont la forme $h+Py$ et qui sont au nombre P^{n-2}. Il reste ainsi $P^{n-2}(P-1)$ valeurs de z dans chacune des formules (a) qui sont au nombre de $\varphi(P-1)$; après cette exclusion, les formules (a) contiennent en tout

$$\begin{aligned} P^{n-2}(P-1).\varphi(P-1) &= \varphi(P^{n-1}).\varphi(P-1) \\ &= \varphi[P^{n-1}(P-1)] = \varphi[\varphi(P^n)] \end{aligned}$$

nombres qui sont racines primitives pour le module P^n, c'est-à-dire qui appartiennent à l'exposant $P^{n-1}(P-1)=\varphi(P^n)$.

Ces assertions se prouvent ainsi qu'il suit :

On partagera les nombres $1, 2, 3, \ldots, P-1$ en deux classes : 1° les nombres $h, h', h'', \ldots$ qui appartiennent à des exposants diviseurs de $P-1$ et plus petits que $P-1$, c'est-à-dire que les nombres $h, h', h'', \ldots$ ne sont pas racines primitives;

2° Les nombres $g, g', g'', \ldots$, qui appartiennent à l'exposant $P-1$, ou les $\varphi(P-1)$ racines primitives pour le module P.

Théorème. — *Si l'on fait $f=h+Pz$, les nombres f appartiendront à des exposants diviseurs de $k.P^{n-1}$ pour le module P^n, en supposant que h appartienne à l'exposant k pour le module* P.

Démonstration. — On a

$$f^k = h^k + Pv.$$

Or on a aussi

$$h^k = 1 + Pu;$$

donc

$$f^k = 1 + Pw;$$

élevant à la puissance P^{n-1}, on aura

$$f^{kP} = 1 + P^2 w', \quad f^{k.P^2} = 1 + P^3 w'',$$

et enfin

$$f^{k.P^{n-1}} = 1 + P^n w.$$

De là on doit conclure seulement que f appartient à un exposant diviseur de kP^{n-1}, f n'appartient donc pas à l'exposant $(P-1).P^{n-1}$, mais à un exposant inférieur.

THÉORÈME. — *Les nombres $f = g + Pw$, qui donnent*

$$(g + Pw)^{P-1} - 1 = Pz,$$

appartiennent à l'exposant $(P-1).P^{n-1}$ *quand z n'est pas divisible par* P; *ils n'y appartiennent pas dans le cas contraire.*

Démonstration.—Les nombres $f = g + Pz$ ne sauraient appartenir aux exposants k, P^{α}_{1}, kP^{α}, le module étant P^n et k diviseur de $P-1$ autre que $P-1$. En effet, on a

$$(g + Pz)^P = g^P + P^2 u.$$

Or $g^{P-1} = 1 + Pv$ donne

$$g^P = g + Pgv;$$

donc

$$(g + Pz)^P = g + Pw;$$

semblablement

$$(g + Pz)^{P^\alpha} = g + Pw'.$$

Si l'on avait

$$(g + Pz)^{P^\alpha} \equiv 1 + P^n . z,$$

on aurait donc

$$g \equiv 1, \quad \text{mod. P},$$

ce qui n'est pas. Comme l'on a

$$(g + Pz)^k = g^k + Pu,$$

supposer

$$(g + Pz)^k = 1 + P^n v,$$

c'est supposer

$$g^k \equiv 1, \quad \text{mod. P},$$

ce qui n'est pas. Même démonstration pour l'exposant kP^α. Ainsi les nombres $g+Pz$ ne peuvent appartenir qu'à l'exposant $(P-1).P^\alpha$, il reste à voir quand on peut prendre $\alpha < n-1$.

Soit $f^{P-1} = 1 + Pz$, z n'étant pas divisible par P; en élevant à la puissance P, on aura

$$f^{(P-1).P} = 1 + P^2 z',$$

où z' n'est pas divisible par P; puis semblablement

$$f^{(P-1)P^2} = 1 + P^3 z'',$$

où z'' n'est pas divisible par P, et ainsi de suite; de sorte qu'il faut élever f^{P-1} à la puissance P^{n-1} pour avoir

$$f^{(P-1)P^{n-1}} = 1 + P^n . z_1,$$

et z_1 n'est pas divisible par P.

Théorème. — *La puissance* $f^{P-1} = (g+Pz)^{P-1}$ *ne peut donner* $(g+Pz)^{P-1}-1$ *divisible par une puissance de* P *supérieure à* P *que quand, en faisant* $g^P = g + hP + kP^2$, *on a*

$$z \equiv h, \quad \text{mod. P}.$$

Démonstration. — Quand $(g+Pz)^{P-1}-1$ est divisible par P^2 ou par une puissance de P supérieure à P^2, il est nécessaire que $(g+Pz)^P - (g+Pz)$ soit divisible par P^2, et quand cela arrive $(g+Pz)^{P-1}-1$ est aussi divisible par P^2; or

$$(g+Pz)P = g^P + P^2 u = g + hP + P^2 . v,$$

donc

$$(g+Pz)P - g - Pz = (h-z)P + P^2 v;$$

il faut donc avoir

$$z = h + Pt.$$

Quand cela arrive, $f^{P-1}-1$ est divisible par P^2; quand cela n'arrive pas, $f^{P-1}-1$ n'est divisible que par P.

Cet énoncé démontre la règle du n° **182**, et l'on a cette proposition :

Théorème. — *Il y a pour le module* P^n *autant de nombres appartenant à l'exposant* $P^{n-1}(P-1) = \varphi(P^n)$ *qu'il y a de nombres inférieurs et premiers à* $\varphi(P^n)$, *c'est-à-dire* $\varphi[\varphi(P^n)]$.

On prouve comme pour le module P ces autres propositions :

THÉORÈME. — *Si le nombre g appartient à l'exposant* $P^{n-1}(P-1)$ *pour le module* P^n, *il en sera de même de* g^i *ou du reste de la division par* P^n *quand i est inférieur et premier à* $P^{n-1}(P-1)$.

THÉORÈME. — *Pour toute racine g appartenant à l'exposant* $P^{n-1}(P-1)$ *pour le module* P^n, *on a*

$$g^{P^{n-1}(P-1)} \equiv 1, \quad g^{\frac{1}{2}P^{n-1}(P-1)} \equiv -1, \quad \text{mod. } P^n,$$

$$g^{\text{in}\,\text{d}a} \equiv a, \quad g^{\text{in}\,\text{d}a \pm \frac{1}{2}P^{n-1}(P-1)} \equiv P - a, \quad \text{mod. } P^n.$$

THÉORÈME. — *La congruence*

$$g^\alpha \equiv g^\beta, \quad \text{mod. } P^n,$$

entraîne

$$\alpha \equiv \beta, \quad \text{mod. } P^{n-1}(P-1).$$

Tout ce qui a été dit des Tables pour le module P s'applique aux Tables pour le module P^n.

Remarque. — Jacobi, dans l'Introduction de son *Canon arithmeticus*, a démontré le premier que toute racine primitive pour le module P^2 l'est aussi pour le module P^α, où α est plus grand que 2. Il restait à donner la manière de trouver les racines pour le module P^2, en supposant connues celles pour le module P : c'est ce que j'ai indiqué dans une Note sur le *Canon arithmeticus* (*Journal de M. Liouville*, t. XIX).

Il y a divers moyens d'abréger le calcul de la racine primitive au moyen de laquelle on construit les Tables. Ils seront indiqués dans l'Introduction d'une Table plus étendue que celle de Jacobi.





